



Guide pour gérer les aspects juridiques du Web 2.0 en milieu scolaire

Pierre TRUDEL et France ABRAN

Équipe de recherche

Cynthia Gaudette
François Joli-Coeur
Annie Lagueux
Geneviève Normand
Jean-François R. Ouellette

2012

Catalogage avant publication de Bibliothèque et Archives nationales du Québec et Bibliothèque et Archives Canada

Trudel, Pierre, 1952-

Guide pour gérer les aspects juridiques du Web 2.0 en milieu scolaire

Comprend des réf. bibliogr.
Publ. en collab. avec: Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique.

1. Internet en éducation - Droit - Québec (Province). 2. Sites Web - Droit - Québec (Province). 3. Sites Web - Développement - Québec (Province). I. Abran, France, 1960- . II. Université de Montréal. Centre de recherche en droit public. III. Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique. IV. Titre.

KEQ923.5.T78 2012 344.714'070285 C2012-941376-3

On peut se procurer une version imprimée de cet ouvrage à :

Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique
Centre de recherche en droit public
Faculté de droit , Université de Montréal
Site internet: www.chairelrwilson.ca
Courriel: france.abran@umontreal.ca
Tél. : (514) 343-2137

Ce guide est également disponible en version PDF sur le site www.droitsurinternet.ca.

ISBN 978-2-922112-04-7 (version imprimée)
ISBN 978-2-922112-05-4 (PDF)

Dépôt légal: 3e trimestre 2012

Table des matières

Introduction

L'expression Web 2.0 renvoie à un ensemble de réalités et de situations qui échappent à une définition qui serait exhaustive[1]. Caractérisé par certains éléments emblématiques, le Web 2.0 renvoie à une constellation de fonctions possédant des caractéristiques communes. Parmi ces caractéristiques, il y a un niveau élevé d'implication des usagers dans la fourniture de contenus. On associe également au Web 2.0 ces environnements structurés dans lesquels les contenus sont générés en bonne partie par les utilisateurs comme les sites d'édition collective, tel celui de l'encyclopédie *Wikipédia*. Ces sites permettent aux internautes d'éditer et de modifier des contenus à leur guise. Dans d'autres cas de figure, on évoque la possibilité de combiner des applications et des contenus et de synchroniser un site web avec d'autres[2]. Les sites de partage de contenus comme *YouTube* ou *Dailymotion* permettent aux internautes de diffuser des contenus en ligne. Les sites de réseaux sociaux comme *Facebook* ou *Myspace* permettent quant à eux aux individus de diffuser leur profil personnel de même que des informations portant sur d'autres personnes[3].

Un auteur observe que la notion de Web 2.0 « désigne la tendance, observée chez certaines entreprises présentes sur le Web, à publier un contenu généré par les utilisateurs plutôt que de recourir au modèle d'affaires traditionnel de mise en ligne de contenus médiatiques propriétaires »[4]. On associe souvent au Web 2.0 différentes approches caractérisées par le partage de contenus, le mixage de ceux-ci et leur réutilisation au gré des initiatives des usagers.

L'utilisation des différents outils du Web 2.0 permet l'accès à un ensemble sans précédent de services de communication et à des informations de toute nature. Toutefois, les activités d'échange, de recherche et de diffusion d'information sur Internet comportent des écueils. À l'instar des autres lieux de vie, Internet implique des risques que les enseignants, les autres membres des écoles et des commissions scolaires, les étudiants et les parents doivent connaître et gérer[5].

---

1 Dion HINCHCLIFFE, « Review of the Year's Best Web 2.0 Explanations' », *Web 2.0 Journal*, 4 janvier 2006, en ligne: <http://web2.sys-con.com/node/165914>.

2 Mary MADDEN et Susannah FOX, « Riding the Waves of 'Web 2.0' - More than a buzzword, but still not easily defined. Pew Internet Project., Backgrounder, 5 octobre 2006, en ligne: <http://www.pewinternet.org/pdfs\ PIP_Web_2.0.pdf>; Lis VEASMAN, « 'Piggy Backing' on the Web 2.0 Internet : Copyright Liability and Web 2.0 Mashups », [2008] 30 *COMM/ENT* 311-337.

3 Steven JAMES, « Social Networking Sites : Regulating the Online 'Wild West' of Web 2.0 », [2008] 2 *Ent. L.R.* 47-50.

4 Nicolas W. VERMEYS, « Chronique-Responsabilité civile et Web 2.0 », *Repères*, juillet 2007, en ligne : <http://rejb.editionsyvonblais.com/> (site consulté le 27 juin 2008).

5 François FILLIETTAZ, *Un enjeu pour l'enseignement – Comprendre l'identité numérique*, Direction des systèmes d'information et service écoles-médias, Département de l'instruction publique, de la

En particulier, il y a des risques de se trouver dans une situation pour laquelle la loi a prévu des exigences, des limites ou des interdits. Au risque de se trouver en situation de contravention aux lois, il importe de savoir identifier de tels risques et de se donner les moyens de reconnaître une situation nécessitant des précautions.

Ainsi, ce guide expose notamment comment déterminer et gérer les risques lors de la mise en place de contenus numériques pour l'éducation[6] et l'utilisation des environnements d'Internet dans le milieu scolaire québécois. On y décrit une méthode afin d'implanter des mécanismes et processus adéquats pour prévenir les comportements problématiques reliés aux différentes activités dans un environnement de réseaux.

Les objectifs, les destinataires, la portée ainsi que la trame générale de la démarche proposée sont présentés dans les paragraphes qui suivent.

L'objectif du guide

Ce guide vise à accompagner les personnes concernées par l'utilisation des outils du Web 2.0 en milieu scolaire afin d'assurer qu'elles se déroulent dans le respect des lois et des principes éthiques reconnus.

À quoi sert ce guide ?

Ce guide identifie et analyse les préoccupations relatives à la conduite des personnes dans les environnements de Web 2.0. Il précise également les exigences à respecter et les précautions à prendre dans le développement et l'exploitation de tels environnements.

Ce guide propose enfin une méthode permettant d'identifier les risques et de mettre en place les mesures nécessaires afin que l'utilisation et le fonctionnement des environnements du Web 2.0 soient en conformité avec les valeurs et les lois applicables au Québec.

À qui est destiné ce guide ?

Ce guide est destiné principalement aux personnes responsables de la mise en place et de la gestion de sites ou d'environnements électroniques dans lesquels se déroulent des activités qui concernent l'univers scolaire. Il sera également utile aux usagers des divers

---

culture et du sport, République et Canton de Genève, version 1.0, janvier 2011, en ligne : <http://icp.ge.ch/sem/prestations/spip.php?article165>.

6 Par contenu numérique pour l'éducation, on entend l'ensemble des logiciels d'édition et de communication ainsi que les données et les informations sur support numérique utiles à une activité d'enseignement ou d'apprentissage. Voir sur cette question Robert BIBEAU, *Des contenus pour l'éducation (Les usages, les besoins et l'offre de contenus numériques pour l'éducation au Québec)*, Direction des ressources didactiques, MEQ, février 2002.

environnements d'Internet. Il fournit des informations sur les risques à gérer et les précautions à prendre par tous ceux qui œuvrent à la conception, au développement et à l'implantation de systèmes d'information destinés à soutenir des échanges entre les personnes.

Quelle est la portée de ce guide ?

Bien que les questions relatives aux risques et aux enjeux juridiques se posent en une multitude de situations dans le monde virtuel ou ailleurs, le présent guide traite principalement des risques les plus courants dans le cadre des échanges prenant place dans des environnements électroniques de type Internet. Ce guide n'est pas un traité de droit. De plus, bien que nous ayons mis beaucoup de soins à identifier les dispositions des lois qui trouvent application dans les situations les plus courantes, ce guide ne constitue en rien un avis juridique. Les conseils qu'il comporte sont de portée générale et ne sauraient remplacer une expertise spécifique dans des cas particuliers.

Nous recommandons d'aborder les dimensions juridiques des principaux services que nous trouvons habituellement dans les lieux proposant un accès à Internet selon une approche de gestion de risques. Le respect des lois n'est pas en soi une question de degré : nous devons évidemment toujours respecter les lois. Toutefois, lorsque des activités relatives à Internet sont mises en place, il est opportun de prévoir les difficultés juridiques susceptibles de découler des activités proposées ou permises, en en évaluant préalablement les risques.

L'approche proposée ici relève d'une démarche par laquelle nous analysons les environnements, les activités de même que les caractéristiques des personnes concernées afin de prendre les mesures préventives qui réduiront les risques de se trouver en contravention avec les lois.

La démarche proposée

Elle se présente en quatre temps :

1. **Situer les responsabilités** : identifier qui fait quoi et qui répond de ce qui se passe lors d'une activité se déroulant sur Internet.
2. **Identifier les risques** : pour cela, il faut partir des activités se déroulant sur Internet sous les auspices de l'institution, de l'école ou de l'organisme.
3. **Évaluer les risques** : une telle évaluation tient compte aussi bien des caractéristiques de l'activité que du fonctionnement ou de la configuration des outils Internet utilisés.
4. Enfin, **identifier et mettre en place des mesures et politiques** qui permettent une prise en charge appropriée des risques.

L'approche générale

Pour devenir compétents dans la société de l'information, les élèves doivent acquérir des compétences relatives à la communication dans les réseaux comme Internet et assumer leurs responsabilités. Ils doivent donc apprendre des façons de faire compatibles avec les principes éthiques en dépit du fait que la technologie leur procure – sans doute à un niveau rarement égalé dans l'histoire – la possibilité d'agir autrement. Il est généralement reconnu qu'il est futile de tenter de leur interdire l'accès aux divers environnements en ligne. Il est plus utile de les former à la gestion des risques inhérents aux environnements d'Internet.

Lorsque des ressources Internet sont fournies par une école ou une commission scolaire, cela doit se faire dans un cadre respectant les principes et valeurs fondamentales tels que reflétés notamment dans les lois. Les personnes ne laissent pas leur droit à la dignité, pas plus que leurs libertés aux portes du cyberespace. Le processus de contrôle et de surveillance des environnements d'Internet ne saurait donc faire fi de la protection des droits des personnes. En revanche, l'accès et l'usage d'Internet ne peuvent s'envisager comme si tout se déroulait dans un cadre toujours pleinement maîtrisé. Il importe aussi de prendre pour acquis que l'usage d'Internet ne peut être envisagé comme une activité qui prend place uniquement dans l'espace contrôlé de l'école.

C'est pourquoi il est souvent insuffisant de décréter des «conditions d'utilisation» et de se réserver simplement le droit de surveiller et de punir. Il est tout aussi contre-productif de multiplier les conditions, contrôles, précautions et processus bureaucratiques sous prétexte d'assurer un environnement protecteur. Sur Internet, le phénomène de la concurrence des régulations joue à plein : les usagers ont plusieurs possibilités de contourner les règles qui ne répondent pas à leurs besoins ou qui sont formulées de manière irrationnelle.

Si les conditions d'utilisation d'un environnement informatique sont perçues comme trop lourdes ou autrement inadaptées aux besoins des acteurs en première ligne, ces derniers ont à leur disposition des services, le plus souvent gratuits et conviviaux, capables de procurer les services ou fonctionnalités recherchées. Mais cela se fait à des conditions qui ne sont pas toujours compatibles avec les exigences qui prévalent ici. Par exemple, si les exigences afin de mettre en place des services de courriel sont mal adaptées ou perçues comme trop lourdes, le risque est grand que les usagers utilisent des outils proposés par les entreprises comme Hotmail ou Yahoo! Toutefois, ces outils pourraient ne pas respecter toutes les exigences qui figurent dans les lois québécoises.

Le défi est de promouvoir effectivement des environnements sécuritaires, non pas en appliquant de façon tatillonne une multitude de limites et de restrictions, mais plutôt en se concentrant sur celles qui assureront les protections fondamentales recherchées. Il faut favoriser un usage informé et responsable plutôt qu'une réglementation caporaliste.

Il existe une certaine croyance voulant qu'il suffise d'installer des filtres ou autres outils afin de filtrer ou autrement contrôler les informations problématiques dans les différentes situations d'Internet. Or, la réalité généralement vécue par les personnes concernées quotidiennement par ces questions est plutôt qu'il est impossible de s'en remettre uniquement à des outils techniques pour faire disparaître les risques et les dangers inhérents à l'usage de plusieurs outils sur Internet.

En l'espèce, plusieurs choix et possibilités d'action sont sous la maîtrise des individus. Il faut donc les informer adéquatement. Il y a des choses qui se règlent plus efficacement au niveau des acteurs directement concernés. C'est pour cette raison que ce guide identifie les responsabilités de chacun des principaux acteurs. Il propose également des outils à l'intention de chacun afin de les aider à décider des mesures à prendre pour gérer les risques qui sont associés à l'une ou l'autre des activités envisagées.

> ***Identifier les caractéristiques de l'outil***
>
> *Internet n'est pas un environnement univoque : plusieurs fonctions et services existent qui ne posent pas les mêmes enjeux. Sur Internet, on peut échanger des messages de courriel entre intimes ou diffuser une chanson à la grandeur du réseau. Les risques doivent donc être appréciés à la lumière des caractéristiques que présentent les différents outils disponibles dans le cyberespace.*
>
> ***Identifier les caractéristiques des participants***
>
> *Les décisions à l'égard des politiques et lignes de conduite doivent tenir compte des besoins des destinataires en fonction de leur âge et de leur besoin de sécurité. Les règles doivent être exprimées dans un langage adapté au niveau de maturité des usagers visés.*
>
> ***Identifier les caractéristiques des activités, évènements prévus et possibles***
>
> *Toutes les activités ne soulèvent pas les mêmes enjeux. Certaines sont anodines et ne posent pas de problèmes particuliers, d'autres par contre nécessitent des précautions plus grandes.*
>
> ***Choisir les politiques et instruments afin de gérer adéquatement les risques***
>
> *Après avoir complété les grilles de questions proposées, le décideur devrait être en mesure de cerner les questions sur lesquelles la politique doit porter. Par exemple, est-il nécessaire d'avoir des dispositions sur la conduite à tenir à l'égard du respect du droit d'auteur ? et quelles sont ces conduites ?*

Les clés de lecture et d'utilisation du guide

Ce guide a été conçu de manière à répondre aux besoins diversifiés de ceux qui ont à prendre des décisions et exercent des responsabilités à l'égard de la mise en place, de la supervision et de la surveillance d'activités prenant place dans des environnements du Web 2.0. Il peut être consulté dans l'ordre de présentation des trois chapitres. Mais il est possible d'aller directement aux chapitres traitant des questions pour lesquelles on recherche des réponses.

Si vous cherchez à identifier et situer les responsabilités que vous avez au sujet de la mise en place, de la surveillance d'activités sur Internet, allez au chapitre I.

Si vous voulez cerner les risques associés aux diverses applications du Web 2.0, allez au chapitre II.

Si vous cherchez des modèles de politiques, des directives, des règlements ou des formules d'autorisations afin de gérer les risques généraux ou spécifiques à certaines activités, consultez le chapitre III.

I- Les responsabilités découlant des activités se déroulant sur Internet

Lorsque nous nous interrogeons sur les responsabilités, nous nous demandons qui est tenu de répondre des situations problématiques qui se manifestent. Nous voulons savoir qui est responsable… qui doit répondre de ce qui ne s'est pas adéquatement déroulé.

Dans ce chapitre, nous expliquons comment sont définies et réparties les responsabilités des enseignants, des écoles, des commissions scolaires, des parents, des étudiants et élèves à l'égard des activités se déroulant sur Internet.

La responsabilité à l'égard des environnements d'Internet se décline à plusieurs niveaux. Dans le monde de l'éducation, cette responsabilité revient ultimement à la commission scolaire du réseau public ou à l'établissement d'enseignement privé. Toutefois, même dans le réseau public, certaines décisions ou actions peuvent être prises au niveau de l'école. Au surplus, l'Internet du Web 2.0 habilite tout usager à diffuser ou à interagir.

Il pourra fréquemment arriver qu'à même les environnements génériques disponibles ou même en dehors de ceux-ci, des enseignants ou des étudiants prennent l'initiative de la mise en place d'outils et d'environnements d'interaction.

Chacune des personnes susceptibles d'interagir en ligne doit donc être au fait des enjeux et des risques associés aux activités qui se déroulent dans le cyberespace. La grande liberté dont jouissent les individus sur Internet emporte pour eux l'obligation de prendre les précautions nécessaires afin de se prémunir contre les risques inhérents à la communication en ligne.

A. Les responsabilités assumées par l'école, la commission scolaire et leurs préposés

L'usage d'Internet pour l'accompagnement d'activités d'apprentissage met en jeu différents types de responsabilités. La commission scolaire, ses écoles de même que les établissements d'enseignement privés assument des responsabilités à différents titres.

Il y a d'abord la **responsabilité politique**. Dès lors que survient un événement déplorable, fut-il un incident isolé, ceux ou celles qui «auraient dû» ou qui «n'auraient pas dû» seront montrés du doigt. Nous sommes ici dans le domaine de la responsabilité politique. Les perceptions de l'opinion publique sont ici cruciales. Il suffirait qu'un incident particulièrement médiatique se produise pour que les médias s'interrogent sur les politiques, ou l'absence de politiques de l'organisme à l'égard des usages d'Internet. Dans ce genre de circonstances, il est important pour l'organisme d'être en mesure d'exposer quelles sont ses lignes de conduite, quelles précautions sont prises, quelles

approches sont privilégiées et quels sont les moyens entrepris afin d'éviter que des incidents se reproduisent.

Un deuxième niveau de responsabilité est évidemment celui de la **responsabilité éducative**. Étant donné que les interactions en réseau sont désormais généralisées, il devient essentiel d'informer et d'éduquer les étudiants ou les élèves sur les usages, pratiques et les règles à respecter dans les environnements d'Internet.

Enfin, se pose la question de la **responsabilité légale** : en cas d'incident, il faut déterminer qui devra répondre des fautes et des dommages. Une fois l'environnement d'Internet d'une institution scolaire mis en place, ou encore lorsque des activités supervisées ou relevant de l'école se déroulent sur Internet, se pose nécessairement la question de savoir «qui» répond de ce qui s'y passe, des faits et des actes qui y surviennent.

Premièrement, les commissions scolaires et les écoles ont une responsabilité en tant qu'éducateurs. En effet, ils ont une responsabilité à titre de commettants pour les fautes de leurs employés. Leurs employés sont en effet des personnes qui se voient confier la garde, la surveillance ou l'éducation d'enfants mineurs. Ils sont donc, tout comme les titulaires de l'autorité parentale, responsables des dommages causés par le fait ou la faute du mineur à moins d'établir qu'ils n'ont commis aucune faute dans la garde, la surveillance ou l'éducation de l'enfant mineur.

Deuxièmement, les enseignants ou les institutions scolaires peuvent avoir à intervenir à l'égard d'activités qui se déroulent entièrement en dehors des cadres de l'école, mais qui ont des conséquences significatives sur ce qui se déroule à l'école ou sur les personnes qui s'y trouvent.

Troisièmement, les commissions scolaires et les écoles sont fréquemment en position d'intermédiaires techniques. Au Québec, la *Loi concernant le cadre juridique des technologies de l'information*[7] (ci-après, la « LCJTI ») prévoit des règles balisant la responsabilité des prestataires de services agissant, à divers titres, en tant qu'intermédiaires dans la recherche, l'hébergement, l'archivage ou la transmission de documents. Ces règles sont énoncées à l'article 22, pour la conservation et la référence à des documents et aux articles 36 et 37 pour la transmission de documents. Ces dispositions précisent les règles permettant de déterminer la responsabilité des intermédiaires techniques.

---

[7] L.R.Q. c. C-1.1, en ligne avec annotations à <http://www.msg.gouv.qc.ca/gel/loi_ti/index.html>.

1. Les responsabilités en tant qu'éducateurs

Les éducateurs, et du coup les commissions scolaires et les écoles, sont responsables du fait de l'enfant mineur. Les articles 1459 et 1460 du *Code civil du Québec*[8] (ci-après, le C.c.Q.) prévoient en effet que les titulaires de l'autorité parentale ainsi que les personnes qui sont chargées de l'éducation d'un mineur sont responsables des gestes posés par les mineurs à l'égard desquels ils exercent une autorité.

La commission scolaire ou l'institution d'enseignement privée est quant à elle le commettant de l'enseignant. Ce dernier agit sous l'autorité de son employeur. L'article 1463 C.c.Q. prévoit que l'employeur est tenu de réparer le préjudice causé par la faute de ses préposés dans l'exercice de leurs fonctions.

Les obligations de prudence qu'il convient de respecter se présentent différemment selon le rôle que l'on tient dans le cadre d'une activité et la place tenue par cette activité dans le projet éducatif. Cette obligation de prudence incombant aux membres du personnel de l'école connaît des variations selon l'âge et les caractéristiques des personnes concernées. S'agit-il de personnes particulièrement vulnérables ou bien de personnes très familières avec les situations et les dangers qui peuvent survenir ?

L'obligation de prudence est aussi fonction des risques inhérents au type d'activités. L'initiateur d'une activité a généralement le devoir d'informer les participants des risques associés à l'activité. Il lui incombera souvent de mettre en garde les participants afin qu'ils ne soient pas pris par surprise.

L'enseignant, l'animateur ou l'initiateur d'une activité éducative sur Internet peut être responsable à deux titres. Premièrement, en participant aux échanges et activités, il est à cet égard tenu aux mêmes devoirs que tous les autres participants. Il a l'obligation d'agir de façon prudente et diligente. Il doit avoir une pratique conforme aux règles de bonne conduite ayant habituellement cours dans le monde de l'enseignement. Deuxièmement, il peut être responsable à titre de gardien ou de surveillant. Alors, il répond des préjudices causés aux tiers pendant que l'élève est sous sa surveillance. Il est aussi possible d'établir que l'acte de l'élève est une conséquence de la mauvaise éducation qu'il a donnée à l'élève.

Il paraît raisonnable de considérer que le devoir de surveillance porte sur l'ensemble des activités se déroulant sur Internet ET qui relève de l'école. Dans le contexte d'Internet, il y a souvent délocalisation du lieu dans lequel s'effectuent la surveillance de même que les activités de formation. L'élève mineur peut poser des gestes dans une situation où l'enseignant n'est pas en mesure d'intervenir. Se pose alors la question de savoir quand commence et quand se termine le devoir de surveillance de l'enseignant.

---

8 L.Q. 1991, c.64.

On peut aussi considérer qu'il existe un devoir de prévenir les parents ou les autres personnes qui sont en mesure d'exercer la surveillance requise et d'intervenir, le cas échéant.

- ***Les limites de la responsabilité***

L'article 1460 C.c.Q. établit une présomption de faute à l'égard des enseignants. Cela est différent d'une présomption de responsabilité. On ne prend pas pour acquis, jusqu'à démonstration contraire, qu'il est responsable, mais on prend pour acquis une faute de sa part jusqu'à ce qu'il démontre qu'il a eu un comportement sans faute. C'est-à-dire le comportement qu'aurait eu, en pareilles circonstances, un enseignant normalement prudent et diligent. C'est pourquoi l'enseignant peut bénéficier de plusieurs motifs d'exonération.

Il faut rappeler que la responsabilité de l'enseignant ne s'étend pas au-delà du temps où dure son obligation de surveillance. L'enseignant a un devoir de surveillance pour la durée du cours, de l'activité ou du laboratoire. Lorsque cette obligation prend fin, la responsabilité prend également fin. Cela signifie qu'il faut prévoir comment est supervisée l'activité pouvant s'étendre au-delà du temps de classe ou pouvant se continuer en dehors de l'école.

L'exonération pourra aussi découler de la démonstration qu'il a exercé une surveillance adéquate. Le caractère adéquat de la surveillance s'apprécie en fonction des circonstances; il tient compte des règles de l'art, des usages du métier et des pratiques généralement suivies ou recommandées dans le milieu professionnel concerné. En pratique, les tribunaux examinent avec attention le système de surveillance de l'établissement.

Un autre moyen d'exonération est l'imprévisibilité de l'acte. L'enseignant peut en effet s'exonérer en montrant qu'en dépit des précautions raisonnables de sa part, le comportement de l'élève ne pouvait être connu de lui ni être prévu. Par contre, l'enseignant qui tolère de façon ouverte ou tacite des comportements dangereux de la part de l'élève sans prendre des mesures pour que cela cesse se verra reprocher de n'avoir pas exercé une surveillance adéquate.

Enfin, on prend en considération les risques inhérents à l'activité. Les tribunaux ne vont pas jusqu'à exiger la prohibition de toute activité dangereuse. Ils imposent l'obligation de ne pas laisser l'élève s'exposer à des risques inutiles ou qui ne sont pas appropriés à son âge et à ses aptitudes. Ainsi, la preuve que des instructions adéquates ont été données sur la façon de prendre part à une activité, de même que des mesures appropriées de sécurité ont été mises en place constituera une démonstration que l'on n'a pas commis de faute.

De ces principes généraux relativement à la conduite diligente que doit avoir un enseignant, il est possible de déduire certaines règles de conduite prudente lors de la tenue d'activités pédagogiques faisant usage d'une composante Internet.

Surveillance adéquate sur les lieux physiques – L'enseignant doit exercer une surveillance adéquate des activités. À l'égard des activités se déroulant en partie sur Internet, il faut distinguer les activités qui supposent des gestes posés en classe, sous l'autorité directe de l'enseignant. À l'égard de ces gestes, l'enseignant a une obligation de surveiller les gestes des élèves. Par exemple, Denis et François Guérard donnent les conseils suivants[9] :

> - *Être présent dans le local en tout temps.*
> - *Être vigilant, surveiller de façon régulière ce que font les élèves.*
> - *Dans la classe, s'assurer que les ordinateurs sont placés de façon à voir les écrans.*
> - *Assigner des places aux élèves qu'ils reprendront à chaque cours afin de repérer plus facilement ceux pouvant causer des problèmes.*
> - *Vérifier les appareils dès la sortie du local.*

L'enseignant doit aussi prévenir les élèves des risques des activités, des précautions qui doivent être prises, des conduites à tenir et celles qui doivent être évitées. Il a le devoir d'intervenir lorsque des gestes préjudiciables sont susceptibles d'être posés.

Surveillance sur les lieux virtuels[10] – Lorsque les activités supposent des gestes posés dans l'environnement Internet, mais à partir de la maison ou de tout autre lieu, le devoir de l'enseignant s'apparente à celui d'un maître de site ou du responsable d'une liste de discussion. Il est de sa responsabilité d'exercer une supervision dans les lieux virtuels sur lesquels il exerce un contrôle. Par exemple, un enseignant qui met en place un forum de discussion doit y prévoir des règles pour le déroulement des échanges et examiner régulièrement les messages qui y sont échangés ou diffusés. Il peut ainsi intervenir rapidement lorsque des actions inadéquates surviennent.

L'obligation d'informer sur les risques – La personne qui organise une activité ou qui y convie d'autres personnes a le devoir d'informer adéquatement ces dernières sur les risques inhérents à l'activité et les façons de s'en prémunir. Afin d'informer des risques afférents à l'utilisation d'Internet, elle doit en expliciter les normes et conditions d'utilisation. Par exemple, l'école peut mettre en place une politique d'utilisation de l'Internet qui lie les élèves et qui est portée à la connaissance des parents.

Les activités se déroulant sur Internet n'ont souvent pas un début et une fin situés dans le temps et dans l'espace comme la plupart des activités scolaires. Par exemple, les

---

9 Denis GUÉRARD et François GUÉRARD, *Clé @ Tic : Guide pratique et activités éducatives*, Montréal, Hurtubise HMH, 2001, p. 98. Voir aussi RÉSEAU ÉDUCATION-MÉDIAS, *Comment réduire les risques en classe*, en ligne : <http://www.reseau-medias.ca/francais/ressources/projets_speciaux/toile_ressources/reduire_risques_en_classe.cfm>.

10 «Se dit d'un lieu, d'une chose, d'une personne, etc., qui n'existent pas matériellement, mais numériquement dans le cyberespace», en ligne : <http://www.granddictionnaire.com>.

différentes activités associées aux réseaux sociaux peuvent avoir lieu le soir. Comme Internet tend à effacer les frontières spatiales et temporelles, il devient difficile de déterminer où commencent et où s'arrêtent les obligations de l'école. Il est tout aussi complexe de situer où commence et où se termine le droit de l'école de prescrire et d'imposer une conduite dans les environnements Internet. Il faut donc développer des façons d'agir qui tiennent compte des caractéristiques d'Internet.

Quelques repères permettent de situer les limites entre ce qui relève de l'école et ce qui relève de la vie privée des personnes. Comme Internet laisse une grande marge de liberté à l'usager, y compris les enfants, il faut une stratégie de sécurisation dépassant le seul cadre des lieux physiques de l'école ou de l'organisme. On comprendra d'entrée de jeu, que s'agissant d'Internet, il est insuffisant de poser, comme on le fait traditionnellement, que les règles de l'école s'appliquent dans l'espace physique de l'institution de même que lors des activités organisées sous l'autorité de l'école. Par contre, il paraît raisonnable de poser que les règles de l'école trouvent application à l'égard de l'ensemble des activités afférentes aux programmes d'études de même qu'aux activités organisées à partir de l'école ou sous ses auspices.

À l'inverse, les initiatives des élèves agissant en dehors de toute démarche scolaire ne relèvent pas de la discipline de l'école.

2. La responsabilité pour les situations présentant une connexité avec l'école

Si *a priori*, la responsabilité de l'école et des enseignants s'applique sur les lieux physiques de l'école, force est de constater que la généralisation des outils du Web 2.0 et la disponibilité accrue d'outils dotés d'importantes capacités de diffusion pose la question de savoir où commencent et où s'arrêtent le droit et la responsabilité de l'école.

En effet, le Web 2.0 modifie radicalement les références spatiales et temporelles. « Avec l'apparition d'Internet puis du Web 2.0, l'institution-école s'est élargie en une communauté de pratique planétaire qui a fait éclater les murs de l'enceinte scolaire et les cadres traditionnels de l'instruction et de l'éducation. »[11] Cette délocalisation accompagnée de la dé-temporisation de l'espace associé à l'école requiert de s'interroger sur les responsabilités des enseignants et des autorités scolaires pour les gestes fautifs commis en dehors de l'espace physique de l'école. Tant aux États-Unis qu'au Canada, les tribunaux ont reconnu que les autorités scolaires peuvent appliquer des sanctions aux enseignants ou aux élèves pour des activités fautives s'étant déroulées sur Internet, et ce, même si les gestes ont été posés entièrement en dehors des espaces relevant de l'école.

---

11 Caroline D'ATABEKIAN et Caroline JOUNEAU-SION (coordonné par), « Le Web 2.0 et l'École - Des enjeux professionnels sensibles », *Les Cahiers pédagogiques*, n° 482, juin 2010, p. 48.

Dans *Ross c. Conseil scolaire du district n° 15 du Nouveau-Brunswick*[12], le juge Laforest écrit que :

> Une école est un centre de communication de toute une gamme de valeurs et d'aspirations sociales. Par l'entremise de l'éducation, elle définit, dans une large mesure, les valeurs qui transcendent la société. Lieu d'échange d'idées, l'école doit reposer sur des principes de tolérance et d'impartialité de sorte que toutes les personnes qui se trouvent en milieu scolaire se sentent également libres de participer. Comme l'a dit la commission d'enquête, le conseil scolaire a l'obligation de maintenir un milieu scolaire positif pour toutes les personnes qu'il sert.

Insistant sur le lien de confiance qui doit exister entre l'enseignant et la collectivité, le juge Laforest explique ainsi qu'il soit possible pour les autorités scolaires d'appliquer des sanctions même pour des gestes qui auraient été posés en dehors du cadre strict de l'institution scolaire. Il écrit[13] :

> C'est en raison de cette position de confiance et d'influence que nous exigeons de l'enseignant qu'il se conforme à des normes élevées au travail comme à l'extérieur du travail, et c'est l'érosion de ces normes qui est susceptible d'entraîner, dans la collectivité, une perte de confiance dans le système scolaire public. Loin de moi l'idée de vouloir ainsi soumettre la vie entière des enseignants à un contrôle démesuré dicté par des normes morales plus strictes. Cela risquerait d'entraîner une violation importante des droits à la protection de la vie privée et des libertés fondamentales des enseignants. Toutefois, lorsque l'«empoisonnement» d'un milieu scolaire est imputable au comportement d'un enseignant après ses heures de travail, et qu'il est susceptible d'entraîner une perte correspondante de confiance dans l'enseignant et dans l'ensemble du système, ce comportement après le travail devient alors pertinent.

Bien que la décision Ross concerne le comportement d'un professeur en dehors de l'espace de l'école, l'on peut retenir que la Cour suprême accorde beaucoup d'importance aux conséquences qu'un comportement hors campus peut engendrer dans la relation éducative. Pour cette raison, les auteurs Shaheen Shariff et Leanne Johnny estiment que cette analyse de la Cour suprême est tout à fait pertinente à l'analyse de comportements fautifs comme le harcèlement commis sur Internet[14].

Aux États-Unis, compte tenu de la protection reconnue par le Premier Amendement aux propos des professeurs et des étudiants, les tribunaux tendent à suivre la position selon laquelle les autorités scolaires ne peuvent appliquer les règles disciplinaires de l'école à l'égard de situations qui présentent à moins de démontrer un lien de connexité suffisant et significatif avec les activités de l'école.

---

12 [1996] 1 R.C.S. 825, par.42.

13 [1996] 1 R.C.S. 825, par.45.

14 Shaheen SHARIFF et Leanne JOHNNY, « Cyber-Libel and Cyber-Bullying : Can Schools Protect Student Reputations and Free-Expression in Virtual Environments ? »,(2007) 16 *Education and Law Journal*, 307-342, p. 334.

Toutefois, dès lors que la connexité entre le propos et les perturbations ressenties dans le milieu scolaire est établie, les tribunaux américains semblent enclins à reconnaître que le pouvoir d'intervention des autorités scolaires ne se limite pas aux frontières géographiques de l'école. Dans *J.S v. Blue Mountain School District*, les juges majoritaires écrivent que :

> We thus cannot overlook the context of the lewd and vulgar language contained in the profile, especially in light of the inherent potential of the Internet to allow rapid dissemination of information. Accordingly, J.S.'s argument for a strict application of *Tinker*, limited to the physical boundaries of school campuses, is unavailing. *See Doninger*, 527 F.3d at 48-49 ("'[T]erritoriality is not necessarily a useful concept in determining the limit of [school administrators'] authority.'" (alteration in original) (quoting *Thomas*, 607 F.2d at 1058 n.13)). Instead, we hold that offcampus speech that causes or reasonably threatens to cause a substantial disruption of or material interference with a school need not satisfy any geographical technicality in order to be regulated pursuant to *Tinker*.[15]

En fin de compte, la délocalisation et la détemporalisation de l'espace scolaire tendent à s'accompagner d'un ajustement conséquent des pouvoirs reconnus aux autorités scolaires de prendre les mesures raisonnablement nécessaires afin de faire cesser des comportements en ligne qui sont de nature à engendrer un effet délétère sur le milieu d'apprentissage de l'école. Par contre, il est moins clair que l'école ou l'enseignant soit tenu à une obligation positive de prendre les mesures afin qu'il soit mis fin à une activité se déroulant totalement en ligne et en dehors de l'établissement, même si cette activité emporte des conséquences significatives sur le milieu de l'école.

3. Les responsabilités en tant qu'intermédiaires techniques

En certaines circonstances, les enseignants, les écoles ou les commissions scolaires peuvent assumer une responsabilité en raison du fait qu'ils agissent comme intermédiaires, c'est-à-dire une **personne qui ne prend pas une part active dans la décision de diffuser des informations sur Internet** ou encore d'accéder à des informations.

Au Québec, la LCJTI prévoit des règles balisant la responsabilité des prestataires de services agissant, à divers titres, en tant qu'intermédiaires dans la recherche, l'hébergement, l'archivage ou la transmission de documents. Ces règles sont énoncées à l'article 22, pour la conservation et la référence à des documents et aux articles 36 et 37 pour la transmission de documents. Ces dispositions précisent les règles permettant de déterminer la responsabilité des intermédiaires techniques.

---

15 593 F.3d 286 (2010), en ligne : <http://www.ca3.uscourts.gov/opinarch/084138p.pdf>; aussi à <http://www.leagle.com/xmlResult.aspx?xmldoc=in%20fco%2020100204110.xml&docbase=cslwar3-2007-curr>.

D'abord, il faut souligner qu'en principe, les intermédiaires techniques n'ont pas d'obligation générale de surveillance. En vertu de l'article 27 de la LCJTI, les intermédiaires ne sont pas tenus de surveiller les contenus qu'ils hébergent ou qu'ils rendent accessibles pour vérifier s'ils sont illicites. Toutefois, dans le cadre de sa mission éducative, l'école et l'enseignant ont un devoir de surveillance. Donc, dans ce cas, il faut distinguer le contenu hébergé de celui qui est sous la supervision des enseignants ou d'autres membres du personnel dans le cadre d'activités scolaires ou parascolaires. L'école a un devoir général de surveillance, mais hors du cadre des activités de l'école, cette obligation s'éteint si elle n'agit qu'à titre d'intermédiaire technique.

Par exemple, si les pages hébergées sont diffusées dans le cadre de la mission éducative de l'école, elle a un devoir d'en surveiller la teneur. Il peut être opportun de mettre en place un processus de révision périodique des signets. Un enseignant qui télécharge en mémoire locale des sites recommandés pour les travaux en classe supervisés de ses élèves doit les vérifier au préalable afin de s'assurer qu'ils ne comportent pas de contenus problématiques. Par contre, si l'organisme scolaire n'est qu'un hébergeur passif, il n'a pas à surveiller ce qui est hébergé sur ses serveurs. Dans quelles circonstances un organisme scolaire peut-il être un intermédiaire ? C'est le cas, par exemple, lorsque le site de l'école héberge les pages personnelles des élèves ou de l'association étudiante. Il peut s'agir de forums de discussion hébergés dans les installations de l'école ou de la commission scolaire. Les commissions scolaires peuvent exploiter des serveurs de courriels ou des listes de discussion. Enfin, il peut s'agir de forums de discussion hébergés dans les installations de l'école ou de la commission scolaire.

Dans ces situations, l'enseignant ou l'école bénéficient de certaines exonérations de responsabilité. C'est-à-dire qu'ils ne sont pas responsables tant et aussi longtemps qu'ils ne jouent qu'un rôle passif dans la diffusion de l'information qui se révèlerait illicite.

B. La responsabilité des parents ou autres titulaires de l'autorité parentale

Lorsque les élèves prennent part à des activités sur Internet en faisant usage d'un ordinateur situé au domicile familial, ce sont les parents qui exercent une surveillance à l'égard des enfants mineurs.

Il leur revient donc, à la lumière des informations mises à leur disposition, d'exercer une surveillance appropriée. Il est donc de bonne pratique d'informer les parents des activités se déroulant sur Internet organisées à partir de l'école et des conditions d'utilisation d'Internet.

> ***Les informations à communiquer aux parents lorsque l'école ou un enseignant organise des activités sur Internet :***
>
> - *Une description de l'activité, ses objectifs, les modalités de son déroulement.*

- *La description de l'activité doit mentionner les risques spécifiques qui y sont associés de même que les précautions prises afin de minimiser les risques.*
- *Un ensemble de recommandations afin de minimiser les risques lors de l'utilisation d'Internet à partir du foyer familial.*

C. La responsabilité du participant, élève ou étudiant

Les élèves et étudiants ont aussi des responsabilités. L'environnement d'Internet laisse une grande marge d'autonomie aux individus. Ceux-ci sont à même de poser des gestes pouvant avoir des conséquences importantes. Par exemple, révéler à la grandeur d'Internet une information sur une personne peut provoquer de graves répercussions. Or, dans la plupart des situations, l'élève ou l'étudiant agit seul sur Internet. Il peut transmettre des informations, accéder à des forums, révéler des informations sur lui-même ou sur d'autres dans des sites de réseaux sociaux, naviguer de manière à accéder à des informations de toute nature.

Sur Internet, les usagers ont depuis longtemps la possibilité d'introduire des contenus en ligne. Ce qui paraît caractéristique du Web 2.0 au plan du droit est le rôle plus actif que jamais tenu par l'usager. L'une des premières habiletés qu'il doit posséder est celle de connaître les responsabilités incombant à une personne qui transmet ou reçoit des informations sur Internet.

Ainsi, la personne ayant personnellement posé le geste fautif est évidemment la première à en assumer la responsabilité. Lorsqu'elle est douée de raison, la personne qui choisit de mettre en ligne une information ou se comporte de manière à exercer un contrôle sur la diffusion de celle-ci assume la responsabilité découlant de son caractère illicite. Mettre des informations en ligne, c'est assumer une fonction éditoriale, c'est publier des informations, les rendre publiques.

Publier signifie communiquer de l'information à des tiers en sachant que cette information sera lue, vue ou entendue. La publication s'effectuant de manière volontaire suppose une connaissance de la teneur de l'information transmise. Dans le contexte d'Internet, la publication peut résulter de la transmission de fichiers, de discussions dans le cadre de conférences électroniques, de l'envoi d'un courriel ou encore par la mise à disposition d'information dans un portfolio numérique ou dans des documents pouvant être transférés via Internet.

Publier entraîne la responsabilité pour les conséquences qui pourraient résulter de cette communication au public ou à un ensemble de personnes.

Au Québec, l'âge de la majorité est fixé à 18 ans. Le mineur peut tout de même exercer certains droits de son propre chef, quoique dans une certaine mesure limitée par la loi. La loi prévoit différents facteurs de détermination de la capacité du mineur d'exercer certains droits et de poser certains actes dans des circonstances données : l'âge, la

faculté de discernement ou l'arrivée d'un événement précis. Par exemple, vers 7 ans, l'enfant est responsable civilement de ses actes selon les tribunaux; à 14 ans, il peut changer de nom, consentir seul à des soins requis par son état de santé, accéder à son dossier médical, poser des actes relatifs à son emploi, son art ou sa profession; à 18 ans, il atteint la majorité.

Aux États-Unis, dans le *Children's Online Privacy Protection Act,* qui s'adresse aux administrateurs de sites susceptibles d'être visités par les enfants, l'enfant est défini comme une personne de moins de 13 ans.

L'article 157 du C.c.Q. prévoit que le mineur peut, compte tenu de son âge et de sa capacité de discernement, contracter seul pour satisfaire ses besoins ordinaires et usuels. L'utilisation d'Internet constitue-t-elle un « besoin ordinaire et usuel » pour un mineur de 12 ans ? Compte tenu de la réalité actuelle, une réponse affirmative est raisonnable.

Ainsi, si l'on peut convenir que l'élève du primaire n'est pas nécessairement doté de la capacité de discernement lui permettant de comprendre et de consentir seul aux conditions d'utilisation d'Internet, on peut faire l'hypothèse qu'à compter du secondaire, l'élève possède la capacité de discernement nécessaire pour lui permettre de consentir seul aux conditions d'utilisation de la plupart des services proposés sur Internet. C'est pourquoi il convient de sensibiliser l'ensemble des élèves à la responsabilité inhérente associée à l'échange et à la diffusion d'information sur Internet en leur faisant signer un code de conduite adapté à leur âge et à leur degré de maturité. De plus, l'élève du secondaire pourrait consentir seul aux conditions d'utilisation du service en signant un contrat d'utilisation tandis que le parent d'élève du primaire reconnaîtrait, dans une notice de réception, qu'il lui revient d'exercer une surveillance lors de l'utilisation d'Internet par son enfant de la maison ou d'un autre endroit.

Pour gérer adéquatement les responsabilités qui lui incombent, le participant à une activité se déroulant sur Internet doit connaître les risques associés à ces activités, se poser les questions appropriées et prendre les précautions adéquates.

> ***Les informations à communiquer aux élèves participants lors d'une activité sur Internet :***
>
> - *Une description de l'activité, ses objectifs, les modalités de son déroulement.*
> - *Une description des risques spécifiques qui y sont associés.*
> - *Une liste de précautions à prendre afin de minimiser les risques.*
> - *Des consignes sur ce qu'il convient de faire en cas de situation problématique.*
> - *Un ensemble de recommandations afin de minimiser les risques lors de l'utilisation d'Internet à partir du foyer familial.*

En guise de conclusion de cette section consacrée à la responsabilité, il est pertinent de citer le document du ministère de l'Éducation et de la Culture de Nouvelle-Écosse intitulé *Politique des écoles publiques en matière d'accès aux réseaux et d'utilisation des réseaux,* en ligne : < http://lrt.ednet.ns.ca/pdf/aup_fr.pdf >. On y départage les responsabilités pour l'utilisation des réseaux du système des écoles publiques. Ces directives indiquent le type de partage de responsabilités qui peut être fait entre le conseil scolaire, l'école, l'enseignant, les parents, l'élève, ainsi que tous les utilisateurs. Bien que ces directives ne s'appliquent qu'en Nouvelle-Écosse, elles peuvent servir de guide. On en trouve ici de larges extraits :

> ***Le conseil scolaire a pour responsabilité***
>
> - *de mettre au point, de mettre en œuvre et de faire appliquer une politique en matière d'accès aux réseaux et d'utilisation des réseaux pour ses utilisateurs, conformément à la présente politique;*
> - *d'informer ses utilisateurs de la politique du conseil scolaire et des rôles et des responsabilités du conseil scolaire en ce qui a trait à la mise en œuvre et à la mise à jour de la politique du conseil scolaire;*
> - *d'offrir des possibilités de perfectionnement professionnel aux enseignants pour les aider à intégrer les services en ligne, y compris le réseau Internet, dans le programme d'études;*
> - *de s'assurer que les réseaux sont utilisés de façon conforme au code de conduite dans les écoles;*
> - *de s'assurer que les comportements importuns sont traités conformément au code de conduite dans les écoles;*
> - *de faciliter la mise en place de comptes d'accès aux réseaux pour les utilisateurs élèves, les enseignants et le personnel des écoles.*
>
> ***L'école a pour responsabilité***
>
> - *de se conformer à la politique du conseil scolaire et de s'assurer du respect de cette politique;*
> - *d'informer les utilisateurs élèves, le personnel du conseil scolaire et les parents des fonctions, des bienfaits et des risques associés à l'utilisation des ressources des réseaux;*
> - *de tenir à jour les dossiers concernant le consentement à publier des renseignements permettant d'identifier l'individu;*
> - *de s'assurer du respect des modalités des conventions de droits d'utilisation entre les fournisseurs de logiciels et l'école;*
> - *de faciliter le perfectionnement professionnel du personnel concernant l'accès aux réseaux et l'utilisation des réseaux dans le cadre du programme d'études.*
>
> ***L'enseignant a pour responsabilité***
>
> - *d'assurer la gestion globale de l'utilisation faite par les élèves d'un réseau dans les matières qui lui sont attribuées ou lorsqu'il se voit attribuer un rôle de surveillance et de donner des instructions aux élèves concernant l'utilisation appropriée du réseau, y compris sur les points suivants :*

- *fournir aux élèves des instructions claires et indiquer clairement les attentes concernant le respect de la politique du conseil scolaire;*
- *s'assurer que l'utilisation des réseaux est conforme aux résultats d'apprentissage visés par le* Programme des écoles publiques*;*
- *faire au préalable l'examen et l'évaluation des ressources pédagogiques incluant des sites Internet avant de recommander leur utilisation aux élèves;*
- *orienter les élèves vers des ressources sur Internet qui ont fait l'objet d'un examen préalable et de recommandations et qui sont intégrées dans le programme d'études et le programme d'enseignement;*
- *superviser l'accès des élèves aux réseaux;*
- *informer les élèves des comportements appropriés en ce qui concerne les droits d'auteur et la propriété intellectuelle et de donner lui-même l'exemple de tels comportements;*
- *avertir les élèves des dangers qu'il y a à rendre disponibles sur Internet des renseignements permettant d'identifier les individus;*
- *respecter la politique du conseil scolaire.*

L'élève a pour responsabilité

- *de respecter la politique du conseil scolaire dans le cadre des activités pédagogiques planifiées;*
- *d'utiliser les réseaux conformément au code de conduite dans les écoles;*
- *de signaler immédiatement à l'enseignant ou à une personne responsable tout contenu ou toute communication importun(e) qui le met mal à l'aise;*
- *de signaler immédiatement à l'enseignant ou à une personne responsable toute tentative faite par une personne que l'élève ne connaît pas pour organiser une rencontre avec l'élève.*

Tous les utilisateurs ont pour responsabilité

- *d'utiliser les réseaux de façon conforme aux politiques et aux procédures du conseil scolaire et aux lois fédérales et provinciales pertinentes;*
- *d'utiliser le réseau de façon responsable et dans le respect de l'éthique, conformément aux fonctions d'éducation et d'information que cette utilisation est censée remplir;*
- *de n'utiliser que les installations qu'ils ont l'autorisation d'utiliser, que ces installations se situent dans l'école publique ou dans un autre endroit, quel qu'il soit*
- *de faire preuve de prudence lorsqu'ils divulguent à toute personne ou tout système électronique des renseignements permettant d'identifier les individus;*
- *de ne publier qu'avec le consentement des personnes concernées des renseignements permettant d'identifier les individus dans des endroits accessibles via Internet;*
- *de ne pas utiliser la technologie, <u>à quelque endroit que ce soit</u>, à des fins d'intimidation ou de harcèlement;*
- *de ne pas être à l'origine de perturbations des réseaux;*
- *de ne pas tenter d'accéder à des documents, des informations ou des fichiers de nature privée ou personnelle appartenant à une autre personne sans l'autorisation préalable de cette autre personne;*
- *de ne pas abîmer, endommager ou désactiver le travail d'une autre personne ou d'un autre organisme;*

> - *de ne pas accéder à des outils technologiques ou des fichiers informatiques en vue de les manipuler, de les modifier ou de tenter de les endommager, de les désactiver ou de les détruire;*
> - *de ne pas consulter, créer ou distribuer des documents, des images ou des formes d'expression pornographiques, obscènes, racistes, sexuellement explicites ou servant à menacer ou harceler quelqu'un;*
> - *de n'utiliser les réseaux qu'à des fins non commerciales et légales qui entrent dans le cadre du système des écoles publiques.*

En somme, tous ceux qui participent à une activité se déroulant en tout ou en partie sur Internet doivent avoir un comportement prudent. Ils doivent agir comme le ferait une personne normalement prudente et diligente placée en semblables circonstances. Autant les parents que les enseignants répondent des fautes commises par les enfants mineurs placés sous leur surveillance.

La question qui se pose est donc celle de savoir ce que constitue un comportement prudent et diligent lorsqu'il s'agit d'activités sur Internet. Cela revient à apprécier les RISQUES associés aux activités et à prendre les PRÉCAUTIONS conséquentes. Les risques associés à une activité sur Internet ne sont pas tous identiques. Il n'existe pas de recette miracle ou de texte prêt-à-porter qui dispenserait de toute précaution. Le chapitre suivant du guide présente une MÉTHODE afin d'apprécier les risques et identifier les mesures de prudence à observer. Il s'agit de dégager les critères de bonnes pratiques et les précautions à prendre afin de minimiser les risques.

II- Les principales applications du Web 2.0

A. Les sites de réseautage social

1. Qu'est-ce qu'un site de réseautage social ?

Les sites de réseaux sociaux offrent un service en ligne qui permet de mettre en relation différentes personnes. Un réseau social est orienté vers le Web 2.0 c'est-à-dire que les visiteurs sont des participants actifs du réseau, et non pas de simples visiteurs de pages statiques.

La mise en relation des personnes constitue la finalité principale des sites de réseaux sociaux. Boyd et Ellison définissent les réseaux sociaux comme des « services Web qui permettent à une personne (1) de créer un profil public ou partiellement public au sein d'un système délimité, (2) de dresser la liste des autres utilisateurs avec lesquels elle est en relation, et (3) de voir et de parcourir sa liste de relations et celle d'autres utilisateurs du système »[16].

Monica Tremblay observe que :

> Ces sites structurent et révèlent des réseaux sociaux établis ou en développement. Ils relient des individus désirant partager leurs intérêts, leurs activités et certains renseignements. Ils offrent aussi un moyen aux individus de communiquer et d'interagir entre eux de manière virtuelle, à l'aide de différents outils en ligne (messagerie instantanée, blogues, etc.).[17]

Les réseaux sociaux comportent habituellement les composantes suivantes à savoir: (1) des outils pour afficher de l'information personnelle dans un profil lié à une personne qui comprend ses intérêts et des renseignements sur sa vie privée, (2) des mécanismes pour permettre des interactions personnalisées et sociales, basées autour d'un profil (recommandations, discussions, blogues, organisations d'évènements sociaux) et (3) des

---

16 Danah M. BOYD et Nicole B. ELLISON, « Social Networks Sites : Definition, History and Scholarship », *J. COMPUTER-MEDIATED COMM.* 13(1), art. 11 (2007), en ligne : <http://jcmc. indiana.edu/vol13/issuel/boyd.ellison.html>. La traduction française de cette définition est tirée de Jennifer BARRIGAR, *La vie privée sur les sites de réseau social analyse comparative de six sites*, Ottawa, Commissariat à la protection de la vie privée, février 2009, en ligne: <http://www.priv.gc.ca/information/ pub/sub_comp_200901_f.cfm#toc3>.

17 Monica TREMBLAY, *Réseaux sociaux sur Internet et sécurité de la vie privée*, Québec, Laboratoire sur les politiques publiques et la mondialisation, ÉNAP, 2010, p. 2, en ligne : <http://www.enap. ca/enapfra/bibliotheque/pub-personnel/publi-tremblay-monica.html>.

outils pour définir les relations sociales afin de déterminer qui a accès aux informations disponibles dans les réseaux sociaux et qui peut communiquer avec qui et comment[18].

Ces sites de réseautage social ont différentes vocations. Ils peuvent servir à agrandir son cercle d'amis (Facebook), à créer des relations professionnelles (LinkedIn, Viadeo), à faire connaître des groupes musicaux (MySpace), à se mettre en relation avec des gens qui partagent les mêmes intérêts (politiques comme Espoir à Gauche, Néthique, Oliceo; culturels comme Flixster), à retrouver d'anciens camarades de classe (Classmates.com), etc. Il suffit de choisir le site qui répond à nos besoins et de s'y inscrire pour être relié à un ensemble indéterminé de personnes.

Il y a deux façons de se joindre à un site de réseautage sur Internet : 1) recevoir un courriel de la part d'un ami qui nous invite à nous inscrire sur le site ou 2) se rendre directement sur le site de réseautage social qui nous intéresse pour remplir le formulaire d'inscription. Certains sites limitent la faculté d'ajouter au réseau en réservant la possibilité de s'inscrire qu'à ceux qui ont reçu une invitation.

Le formulaire d'inscription permet en général de créer un profil de base, qui peut contenir le nom, la ville de résidence ainsi que l'occupation. Par la suite, il est possible de compléter les informations personnelles de façon plus détaillée, en ajoutant une photographie, un curriculum vitae ou encore des centres d'intérêt. Ces renseignements sont regroupés dans un espace personnel.

Une multitude de services sont disponibles sur les sites de réseaux sociaux. Certains n'offrent qu'un outil de recherche pour rejoindre des individus alors que d'autres offrent de créer un blogue, de mettre en ligne du contenu diffusé en transit, de publier des commentaires, etc. De plus, ces sites procurent plusieurs avantages à leurs membres: un sentiment de connectivité et d'intimité plus souvent par rapport à une communauté hors ligne, mais également face à une nouvelle communauté en ligne. Certains outils permettent aux usagers partageant des points communs de se découvrir mutuellement et d'interagir. D'autres outils font en sorte que les usagers ont le contrôle sur le contenu qu'ils ont créé (ce qui n'est pas permis par les blogues par exemple)[19].

a. Qui fait quoi ?

Les réseaux sociaux mettent des personnes en relation. Les usagers y tiennent donc un rôle majeur. Mais, les entités qui contribuent à faire des réseaux sociaux les

---

[18] EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, « Security Issues and Recommendations for Online Social Networks », *ENISA Position Paper n° 1,* octobre 2007, en ligne : <http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks> (site consulté le 11 mars 2011).

[19] EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, « Security Issues and Recommendations for Online Social Networks », *ENISA Position Paper n° 1,* octobre 2007, en ligne : <http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks> (site consulté le 12 mai 2010).

environnements virtuels qu'ils sont, assument aussi des obligations et génèrent leur part d'enjeux et de risques.

i) Les usagers

Dans les sites de réseaux sociaux, les usagers tiennent des rôles décisionnels. Ils ont à leur disposition différentes fonctions leur permettant de consigner et de diffuser des informations en ligne. Ces informations peuvent porter sur eux-mêmes ou encore sur des tiers.

Toutefois, l'essence même des réseaux sociaux est la représentation des personnes et leur mise en relation. Dans ces environnements, les usagers se révèlent et publient des informations sur eux-mêmes; ils possèdent la faculté de rendre disponibles un vaste ensemble d'informations. En plus, les usagers sont en interaction : ils sont en mesure d'établir des interactions un à un ou avec un ensemble de personnes. C'est donc bien de réseaux qu'il s'agit : Grimmelman explique que « Social networks sites make the graph structure of social networks explicit; users are nodes and connections are links ».

Les réseaux sociaux fixent l'âge minimal pour devenir membre à 13 ans[20]. Hormis le recours à des modes de vérification en ligne de l'identité qui garantiraient que la personne se trouvant en ligne est effectivement celle qu'elle prétend être, il demeure très difficile d'obtenir de la certitude quant à l'âge d'une personne. De plus, il appert que plusieurs approches de vérification de l'âge peuvent comporter plus d'inconvénients que d'avantages, notamment au regard des risques de leurre et d'abus commis à l'endroit de personnes mineures[21].

Les usagers jouent donc un rôle primordial dans la croissance du réseau social. Ainsi, le blogue de Facebook rapportait que le réseau comptait 1 million d'usagers en 2004. Ce chiffre a grimpé à 5.5 millions en 2005, pour pratiquement doubler en 2006 avec 12 millions d'usagers. En octobre 2007 le réseau rejoignait 50 millions de personnes et ce chiffre doubla encore avant le mois d'août 2008. Des sommets inégalés ont été atteints en 2009 alors que le nombre d'usagers a grimpé à 350 millions en décembre pour ensuite continuer d'augmenter au début de 2010 pour atteindre 500 millions en juillet[22]. En août 2011, il y a plus de 750 millions d'usagers actifs sur Facebook.

L'usager qui possède un compte sur un site de réseau social dispose d'espaces privatifs et d'espaces virtuels qui sont accessibles par un ensemble plus ou moins étendu selon

---

20 MySpace, « Conseils et paramètres de sécurité MySpace », en ligne : <http://www.myspace.com/ index.cfm?fuseaction=cms.viewpage&placement=safety_pagetips> (site consulté le 13 mai 2010).

21 Voir : Adam THIERER, *Social Networking and Age Verification: Many Hard Questions; No Easy Solutions, Progress on Point*, The progress & Freedom Foundation, March 2007, en ligne: <www.pff.org/ issues-pubs/pops/pop14.5ageverification.pdf >.

22 Facebook, « Pressroom, Company Timeline», en ligne : <http://www.facebook.com/press/info. php?timeline> (site consulté le 29 août 2011).

les configurations du site ou selon les choix de l'usager. Par exemple, sur Facebook, le profil d'un membre est constitué d'un « mur » comportant une nomenclature d'informations sur l'individu membre, des photos, des liens vers d'autres contenus et autres renseignements indiqués par le membre titulaire du compte. La plateforme génère aussi de façon automatique une liste d'activités récentes en relation avec le compte. Enfin, des tiers peuvent publier des informations qui pourront apparaître sur les pages du titulaire du compte.

L'usager peut configurer son compte de façon à rendre accessibles les informations qui s'y trouvent à un cercle plus ou moins étendu. Par exemple, sur Facebook, les paramètres de confidentialité permettent à l'usager de déterminer si les différents types de contenus seront accessibles à tout le monde, uniquement à leurs « amis » ou encore aux amis de leurs amis. Facebook propose aussi l'option de personnaliser les configurations de manière à rendre accessibles ou non certaines catégories d'information même à l'égard d'un groupe ou de certaines personnes.

Pour profiter de la mise en relation avec d'autres personnes, les usagers peuvent ajouter des contacts, notamment à partir de leur carnet d'adresses. Il est possible de rechercher des individus qui sont déjà membres du site et de leur envoyer des demandes de mise en relation. Si un membre souhaite prendre contact avec quelqu'un qui n'est pas membre, il peut lui envoyer un courriel l'invitant à s'inscrire et à prendre contact. Certains sites vont offrir d'importer la liste de contacts d'une adresse de courrier électronique déjà existante dans le but d'envoyer à toutes ces personnes des courriels d'invitation. Si les personnes concernées se joignent au site, elles apporteront à leur tour leurs contacts et le réseau grandit de cette façon.

Entre eux, les « amis » ou contacts au sein du réseau social peuvent se trouver en situation de constituer un « dossier » sur leurs contacts respectifs. Leur faculté de se livrer à pareille activité dans le contexte des réseaux sociaux est encadrée par l'article 37 du *Code civil du Québec* qui dispose que :

> Toute personne qui constitue un dossier sur une autre personne doit avoir un intérêt sérieux et légitime à le faire. Elle ne peut recueillir que les renseignements pertinents à l'objet déclaré du dossier et elle ne peut, sans le consentement de l'intéressé ou l'autorisation de la loi, les communiquer à des tiers ou les utiliser à des fins incompatibles avec celles de sa constitution; elle ne peut non plus, dans la constitution ou l'utilisation du dossier, porter autrement atteinte à la vie privée de l'intéressé ni à sa réputation.

Ainsi, le fait de constituer une collection de photos d'une personne, ou de réunir des informations relatives à une personne dans un réseau social est, en droit québécois, assujetti à la condition que cela réponde à un intérêt « sérieux et légitime ». L'objet du dossier devrait être déclaré et le droit de communication aux tiers est conditionnel au consentement de l'intéressé.

ii) Les « contacts » et « amis »

Les « contacts » ou « amis » désignent des personnes avec lesquelles un usager entretient une relation plus spécifique. Les relations peuvent être symétriques : par exemple, sur Facebook les relations entre « amis » sont symétriques. Si je suis votre ami, vous êtes nécessairement mon « ami ». D'autres sites de réseaux sociaux permettent d'établir des rapports asymétriques[23]. Le fait d'être en relation dans le contexte d'un réseau social n'est pas en soi une preuve de liens d'affection ou d'intimité. C'est tout au plus un indice d'une intention de demeurer en contact avec les personnes faisant partie de la liste que constitue l'usager[24].

iii) Les « communautés »

Les sites de réseaux sociaux permettent l'établissement de « communautés », c'est-à-dire des ensembles plus ou moins étendus de personnes réunies autour d'intérêts qui peuvent avoir un caractère universel ou encore ne concerner qu'un ensemble restreint d'individus. Des cercles de nature variable se constituent et partagent des intérêts et des informations. Au sein d'un cercle en particulier, un type d'information peut n'avoir qu'une signification banale alors qu'elle prendra un autre sens si elle est partagée avec des personnes se trouvant dans d'autres cercles.

La recherche de relations sociales constitue une motivation inhérente de la participation à des sites de réseaux sociaux. Grimmelman rappelle que « these social urges can't be satisfied under conditions of complete secrecy. Identity performance requires an audience; relationships are impossible without others; community is a public ».[25]

Ainsi, les usagers des sites de réseaux sociaux s'inscrivent dans le cadre d'environnements possédant un caractère collectif. Participer à un site de réseau social suppose nécessairement une volonté de partager des informations avec d'« autres ». Par contre, ces « autres » participants peuvent se trouver au sein de communautés différentes les unes des autres. Ils peuvent aussi avoir des conceptions différentes de ce qui est acceptable, légitime, correct ou incorrect.

iv) Les développeurs

Outre les usagers et les amis, les développeurs jouent un rôle important. Ces derniers créent de nouvelles applications à partir des données inscrites dans les profils des membres des réseaux sociaux. Ainsi, ils se baseront sur l'activité professionnelle, les contacts et l'activité du profil des membres partout dans le monde. Pour *Facebook*

---

23 James GRIMMELMAN, « Saving Facebook », [2009] 94 *Iowa L. Rev.,* 1138, p. 1143.

24 Nicolas W. VERMEYS, « L'admissibilité en preuve de contenus issus de sites de réseaux sociaux», (2010) *Repères* EYB2010REP962.

25 James GRIMMELMAN, « Saving Facebook », [2009] 94 *Iowa L. Rev.,* 1138, p. 1159-1160.

seulement, il y a plus de 950 000 développeurs d'applications provenant d'environ 180 pays[26].

Or, si on se base sur le mode de fonctionnement du réseau Facebook, quand les usagers ajoutent une application (quelle qu'elle soit; jeu, questionnaire ou petite annonce) à leur page personnelle, ils consentent aussi à ce que les développeurs aient accès à leurs renseignements personnels ainsi qu'à ceux de leurs amis. Dans ces cas, l'unique moyen de refuser une telle communication lorsque des amis ajoutent une application est de refuser toutes les applications ou de bloquer des applications particulières[27].

Cela a posé problème pour la Commissaire à la vie privée du Canada qui a recommandé que « Facebook mette en œuvre des mesures techniques pour faire en sorte que les développeurs aient uniquement accès aux renseignements des utilisateurs qui sont essentiels au fonctionnement de l'application »[28]. De plus, la Commissaire a demandé à Facebook de « s'assurer que les utilisateurs sont informés des renseignements précis exigés par l'application et des fins pour lesquelles on recueille ces renseignements »[29]. Ces recommandations ont été refusées par Facebook.

Pour sa part, le Groupe de travail « Article 29 » sur la protection des données estime que :

> Les fournisseurs d'application peuvent aussi être responsables du traitement des données s'ils développent des applications qui s'exécutent en complément de celles des sites de réseaux sociaux et si les utilisateurs décident de s'en servir.[30]

v) Les sites de réseaux sociaux

Les sites de réseaux sociaux les plus fréquentés ont été développés aux États-Unis. Dans une grande mesure, leur fonctionnement reflète les traits du droit américain, notamment quant à la place respective que tiennent la liberté d'expression et d'autres intérêts comme le droit à la vie privée. Ainsi, dans la mesure où les informations se

---

26 COMMISSARIAT À LA VIE PRIVÉE DU CANADA, « Facebook doit améliorer ses pratiques en matière de protection de la vie privée, selon les résultats d'une enquête », Communiqués, en ligne : <http://www.priv.gc.ca/media/nr-c/2009/nr-c_090716_f.cfm> (site consulté le 11 mai 2010).

27 COMMISSARIAT À LA VIE PRIVÉE DU CANADA, « Facebook doit améliorer ses pratiques en matière de protection de la vie privée, selon les résultats d'une enquête », Communiqués, en ligne : <http://www.priv.gc.ca/media/nr-c/2009/nr-c_090716_f.cfm> (site consulté le 11 mai 2010).

28 COMMISSARIAT À LA VIE PRIVÉE DU CANADA, « Facebook doit améliorer ses pratiques en matière de protection de la vie privée, selon les résultats d'une enquête », Communiqués, en ligne : <http://www.priv.gc.ca/media/nr-c/2009/nr-c_090716_f.cfm> (site consulté le 11 mai 2010).

29 COMMISSARIAT À LA VIE PRIVÉE DU CANADA, « Facebook doit améliorer ses pratiques en matière de protection de la vie privée, selon les résultats d'une enquête », Communiqués, en ligne : <http://www.priv.gc.ca/media/nr-c/2009/nr-c_090716_f.cfm> (site consulté le 11 mai 2010).

30 GROUPE DE TRAVAIL, « Article 29 » sur la protection des données, *Avis sur les réseaux sociaux en ligne*, 12 juin 2009, en ligne :< http://ec.europa.eu/justice_home/fsj/privacy/index_fr.htm>. p. 5.

trouvant sur les pages d'un site de réseau social émanent des usagers ou de tiers, la législation américaine exclut que les gestionnaires de ces sites puissent être trouvés responsables de ces informations.

En Europe, la position du Groupe de travail « Article 29 » sur la protection des données reflète la nette préférence du droit européen pour la protection de la vie privée. Pour ce groupe d'experts de l'Union européenne, les sites de réseaux sociaux « sont responsables du traitement des données conformément à la directive sur la protection des données »[31].

Pour ce qui est du droit québécois, selon la *Loi concernant le cadre juridique des technologies de l'information*, les réseaux sociaux présentent les caractéristiques de prestataires offrant « des services de conservation de documents technologiques sur un réseau de communication » ou encore « des services de référence à des documents technologiques, dont un index, des hyperliens, des répertoires ou des outils de recherche » tels qu'envisagés à l'article 22.

Ainsi qualifiés, ces prestataires ne sont pas tenus à une obligation de surveillance active[32]. La possibilité d'engager leur responsabilité naît lorsqu'il est établi qu'ils ont la connaissance de fait ou la connaissance de circonstances rendant apparente la réalisation d'une activité à caractère illicite sur leur site.

b. Utilisation des réseaux sociaux en éducation

Un site de réseau social, comme Facebook, regroupe de nombreuses fonctionnalités. Il permet de communiquer directement avec les autres utilisateurs, par messages privés (semblables au courriel) ou publics (dépendamment des paramètres de confidentialité choisis). Il permet d'opérer un blogue, c'est-à-dire de publier des billets. Également, cet outil sert à publier du contenu multimédia, soit des images, de la musique et des vidéos.

L'établissement d'enseignement, l'enseignant et les élèves peuvent tous se créer un compte sur un réseau social. L'école peut créer un groupe destiné à informer les parents, comme s'ils utilisaient un blogue. Les enseignants peuvent créer une page, afin de tenir les parents informés de l'actualité de leur classe. Toutefois, dans ces deux cas, les pages devront être publiques puisque l'ensemble des parents ne possède pas un compte sur ledit réseau social.

L'enseignant pourrait également utiliser un réseau social pour communiquer avec ses élèves. Par exemple, sur Facebook, l'enseignant pourrait se créer un profil destiné exclusivement à interagir avec ses élèves – de façon à séparer sa vie privée - et les élèves feront de même. De plus, Facebook permet de gérer la confidentialité de la page

---

31 GROUPE DE TRAVAIL, « Article 29 » sur la protection des données », Avis sur les réseaux sociaux en ligne, 12 juin 2009, en ligne : <http://ec.europa.eu/justice_home/fsj/privacy/index_fr.htm>. p. 5.

32 *Loi concernant le cadre juridique des technologies de l'information*, L.Q. 2001, c.32, art. 27.

ainsi créée afin d'éviter un mélange d'informations. Ces paramètres pourront être personnalisés aux objectifs d'un groupe. Les élèves peuvent également se créer des groupes afin de développer un projet. Notamment, un petit groupe d'étudiants qui doit effectuer un travail d'équipe pourrait se créer un groupe, auquel seuls eux-mêmes et leur enseignant auraient accès. De plus, élément particulièrement utile lors de travaux d'équipe, Facebook permet le partage de contenu visuel et audio en plus des messages transmis au moyen de la fonction de messagerie.

L'utilisation des réseaux sociaux et des blogues en éducation offre sensiblement les mêmes possibilités. Par contre, un réseau social comme Facebook est une communauté, un réseau de personnes et il est possible, sous réserve des options de confidentialité, de savoir qui connaît qui… Et pour être membre de Facebook, il faut avoir au moins 13 ans et accepter des conditions d'utilisation, ce qui n'est pas le cas pour les blogues.

2. Quels sont les risques associés aux sites de réseautage social ?

Les réseaux sociaux offrent des fonctionnalités permettant aux usagers d'interagir et d'organiser leurs interactions. Les usagers doivent effectivement avoir la maîtrise de l'information qui les concerne. En contrepartie, ils doivent être en mesure d'assumer les risques résultant des décisions qu'ils prennent à l'égard des informations qu'ils traitent.

Cependant, développer des habiletés sociales en ligne peut constituer un défi plus difficile à relever que le développement d'habiletés dans la « vraie » vie non virtuelle. Contrairement aux voies ordinaires de rencontres en face à face, les conversations en ligne ne permettent pas de percevoir les réactions de l'interlocuteur. L'adolescent ne peut donc pas moduler sa conduite selon les indications qu'il reçoit de son interlocuteur[33].

Certains risques liés aux réseaux sociaux paraissent considérables pour les jeunes. Les sites de réseautage social sont extrêmement populaires auprès des jeunes et leur permettent d'accéder à des canaux indépendants et non supervisés d'expression de soi et de socialisation[34]. Les sites de réseautage social créent également une certaine dépendance[35]. Les risques associés à une plus grande utilisation d'Internet varient de l'interférence avec les études ou autres activités des jeunes à un risque plus élevé de

---

33 Susan HANLEY DUNCAN, « MySpace is Also Their Space : Ideas for Keeping Children Safe from Sexual Predators on Social Networking Sites », (2008) 96 *Kentucky Law Journal*, 540.

34 Susan HANLEY DUNCAN, « MySpace is Also Their Space : Ideas for Keeping Children Safe from Sexual Predators on Social Networking Sites », (2008) 96 *Kentucky Law Journal*, 527.

35 Rhonda GOETZ, « Is MySpace Stealing Your Child's Future », 18 janvier 2006, en ligne : <http://ezineacticles.com/?Is-MySpace-Stealing-Your-Childs-Future?&id=130750&opt+print> cité dans Susan HANLEY DUNCAN, « MySpace is Also Their Space : Ideas for Keeping Children Safe from Sexual Predators on Social Networking Sites », *Kentucky Law Journal*, 96, 2008, p. 539. L'auteur renvoie également à K.S. YONG, « Internet Addiction : The Emergence of a New Clinical Disorder », 19980 I (3), *Cyberpsychologie* 237.

sollicitation en ligne. La dépendance amplifie la possibilité pour les prédateurs sexuels de solliciter les mineurs en ligne. En plus de quoi les adolescents sont plus à même de s'engager dans un comportement plus dangereux[36].

Mais surtout, les réseaux sociaux peuvent donner aux jeunes un faux sentiment de sécurité ce qui mène à un trop grand partage d'informations. Cette perception erronée semble avoir été causée par la méconnaissance du caractère public de ce que les jeunes publient et l'ignorance de l'étendue des étrangers qui peuvent avoir accès à ce qui a été publié. Aussi, les jeunes peuvent penser que les actions posées en ligne sont séparées de celles de la « vraie » vie et finalement, ils semblent croire que le partage d'informations personnelles est la norme dans les réseaux sociaux, comme d'autres usagers le font[37]. Aussi, les jeunes se voient réconforter dans l'anonymat que leur donnent les réseaux sociaux et ressentent un certain sentiment d'impunité pour les actions « virtuelles » qu'ils accomplissent.

Les principaux risques que révèle l'observation du fonctionnement des sites de réseaux sociaux ont trait à la protection de la vie privée. Ainsi, la diffusion devenue très facile de renseignements sur les personnes accentue les risques découlant de la circulation de renseignements sur les personnes en dehors de cercles délimités. Mais la diffusion d'informations de toute nature peut engendrer des risques de harcèlement ou de vol d'identité. De plus, l'information se trouvant consignée dans les environnements de réseaux sociaux peut être décontextualisée et être utilisée à des fins qui n'auront pas toujours été anticipées.

a. La divulgation de renseignements personnels

La diffusion d'informations sur soi ou portant sur d'autres personnes emporte des risques pour la vie privée. Plusieurs réseaux sociaux ont le potentiel de briser les lignes séparatrices entre ce qui est tenu pour être privé ou partagé uniquement dans un cercle limité et les informations disponibles à un plus large public.

Par exemple, dans un site de réseautage social, il est possible de publier des renseignements nous concernant, mais aussi des renseignements concernant nos contacts. De telles informations peuvent être dévoilées lors de la rédaction d'un commentaire. Nos contacts peuvent également mettre des renseignements nous concernant dans leurs sites personnels. Ces sites amènent souvent à dévoiler des coordonnées telles que l'adresse de résidence, les numéros de téléphone et l'adresse de courrier électronique. Les usagers peuvent également y mettre des photographies, qui sont parfois compromettantes.

---

[36] Susan HANLEY DUNCAN, « MySpace is Also Their Space : Ideas for Keeping Children Safe from Sexual Predators on Social Networking Sites », (2008) 96 *Kentucky Law Journal*, p. 539.

[37] Sander J.C. VAN DER HEIDE, « Social Networking and Sexual Predators : The Case for Self-Regulation », 31 *Hastings Comm. & L.J.*2008 180.

Si plusieurs de ces informations prises isolément ont habituellement un caractère anodin, le potentiel pouvant découler de la combinaison de ces informations avec d'autres renseignements disponibles dans les pages personnelles d'un site de réseau social peut devenir préoccupant.

En effet, les environnements de réseaux sociaux rendent très facile le jumelage de renseignements relatifs à une personne et par conséquent la possibilité de révélation indirecte d'informations personnelles, dont certaines pourraient constituer des révélations sur la vie privée. Par exemple, les allusions aux endroits fréquentés ainsi que des informations sur les allées et venues d'un usager ou de ses amis pourraient générer des révélations allant au-delà de ce que la personne concernée par les informations aurait souhaité partager.

Questions à vérifier

- *Le participant est-il amené à dévoiler des renseignements personnels sur lui-même ou sur une autre personne ?*
- *Le participant est-il au courant des risques inhérents à l'utilisation de cet outil ?*
- *Est-ce qu'il y a un contrôle sur l'âge des participants ?*

b. L'utilisation non autorisée de l'image d'une personne et les atteintes au droit d'auteur

Sur les sites de réseautage social, il y a un risque d'atteinte au droit d'auteur. Certains sites offrent de partager du contenu à l'intérieur des espaces personnels. Par exemple, un individu pourrait publier des vidéos contenant des sketches d'un humoriste sans son consentement. Cette diffusion de contenu peut donc constituer une atteinte au droit d'auteur d'un artiste.

Les sites de réseaux sociaux permettent de diffuser des images de personnes ou d'objets. Les enjeux relatifs à la diffusion des images concernent évidemment les droits de propriété intellectuelle pouvant exister sur celles-ci, mais ils mettent aussi en jeu le droit des personnes de s'opposer à la diffusion de leur image sans leur consentement ou en dehors de circonstances où la diffusion serait justifiée par l'intérêt public ou par l'intérêt que pourraient avoir certains proches. Par exemple, utiliser des photographies de nos contacts au sein d'un album en ligne peut constituer une atteinte au droit à l'image d'une personne lorsqu'elle est faite sans son consentement. Le risque peut être accru en raison de la relative facilité à identifier de façon précise une personne figurant sur une image.

Du contenu de nature personnelle ou relevant du cercle intime d'une personne peut se retrouver sur des sites de réseaux sociaux, tels des vidéos de fêtes ou encore de sorties entre amis. Ces vidéos peuvent brimer le droit à l'image de quelqu'un s'il est possible d'identifier la personne filmée. Il n'est même pas nécessaire d'utiliser l'image réelle de cette personne pour transgresser ses droits. En effet, l'utilisation d'un sosie dans une

vidéo et la mention du nom de la personne imitée peuvent suffire à violer le droit à l'image.

Il faut donc s'assurer, avant de publier une image sur Internet, d'avoir les autorisations nécessaires des personnes qui s'y retrouvent, ou qui y sont représentées.

> ***Questions à vérifier***
> - *Est-ce que le contenu contient des œuvres ou parties d'œuvres qui sont protégées par la Loi sur le droit d'auteur ?*
> - *Est-ce que la personne qui diffuse l'information détient les autorisations nécessaires pour la publier ?*
> - *Est-il possible de garder une copie des documents audio ou vidéo ? Internet regorge d'outils permettant d'intercepter et d'enregistrer un flux de sons ou d'images pour les divers formats utilisés.*
> - *Est-ce que le contenu visionné contient des images de personnes identifiables ?*

c. Les atteintes à la réputation

Dans les réseaux sociaux, il est facile de parler de soi et des autres et de conférer à de tels propos une diffusion pratiquement universelle. Or, les mécanismes qui assurent la protection du droit à la réputation des personnes tiennent en compte le contexte de la diffusion du propos et apprécient son caractère diffamatoire par rapport au sens qui est donné au propos, compte tenu de l'ensemble des circonstances de sa diffusion. C'est ainsi que l'on peut trouver licite un commentaire formulé en cercle restreint sur les faits et gestes d'une personne dans le cadre de l'exercice de ses fonctions. Mais le même commentaire porté à l'attention d'un tiers non concerné pourra avoir un caractère diffamatoire ou même haineux en changeant de contexte.

L'atteinte à la réputation sur les réseaux sociaux est particulièrement importante et a un impact direct sur la vie des usagers qui se voient confrontés à de telles situations. La publication d'informations sur Internet a des répercussions qu'il est possible de ressentir immédiatement, mais aussi dans le futur[38]. Une telle atteinte peut se faire par la propre faute des usagers qui communiquent des informations pouvant se révéler dommageables, mais aussi par le biais des autres usagers qui peuvent se méprendre sur les risques associés à la rediffusion de certains éléments d'information préalablement diffusés dans un contexte spécifique.

> ***Questions à vérifier***
> - *Est-ce que les faits présentés sur les espaces personnels sont vérifiés et vérifiables ?*
> - *L'usager nomme-t-il les personnes visées par ses commentaires ?*
> - *Critique-t-il une pratique ou s'adonne-t-il plutôt à des attaques personnelles ?*

[38] Sheerin N.S. HAUBENREICH, « Parental Rights in MySpace : Reconceptualizing the State's Parens *Patriae Role* in the Digital Age », 31 *Hastings Comm. & Ent. L.J.* 223, 2008-2009.

d. Les propos haineux et les menaces

Vu la quantité et la diversité des informations que l'on peut retrouver sur les sites de réseautage social, des personnes mal intentionnées peuvent se servir de ces renseignements dans un but illicite, par exemple, en ciblant quelqu'un pour lui envoyer des menaces ou écrire des propos haineux ou diffamants par rapport à cette personne ou à un groupe de personnes[39].

Une personne peut également produire un profil sur une autre personne et publier des messages diffamatoires ou encore des informations mensongères. Par exemple, un élève pourrait créer un profil sur son directeur d'école et y insérer de fausses informations sur son orientation sexuelle et y écrire des propos menaçants.

De plus, le contenu publié sur le site peut être réutilisé à mauvais escient par des personnes. Par exemple, si quelqu'un envoie une photographie osée à un contact ou la met en ligne, le contact peut s'en servir ensuite pour harceler la personne en question. Il peut la menacer d'envoyer la photographie à des proches, dans le but de salir sa réputation ou d'obtenir d'autres photographies d'elle.

À New York, un homme de 25 ans fait face à des accusations suite à des menaces proférées contre une adolescente. Il l'aurait ainsi forcée à utiliser une caméra Web pour capter des images explicites d'elle-même, images que l'homme a par la suite publiées sur MySpace. Il a rencontré la jeune fille par le biais d'un site de clavardage destiné aux meneuses de claque et lui a ensuite envoyé des messages sexuels explicites. Il l'aurait menacé de la blesser elle et sa famille si elle ne s'exposait pas avec la caméra Web. La jeune fille a fait ce qu'il demandait. Elle a par la suite trouvé les images sur MySpace et a avisé ses parents. L'homme avait ouvert un compte sur le réseau social au nom de la jeune et y avait mis les images obtenues par le biais de la caméra Web[40].

Questions à vérifier

- *Est-ce qu'il y a présence de surveillance sur le site ?*
- *Quel est le sujet traité sur l'espace personnel ? Quel contenu y retrouve-t-on ?*
- *Sommes-nous appelés à révéler des renseignements personnels sur notre espace personnel ?*
- *L'usager encourage-t-il à la haine ou le mépris d'un individu ou d'un groupe identifiable ?*

39 Voir Tristan PÉLOQUIN, « Six élèves suspendus pour un site Web diffamatoire », *La Presse*, 16 mai 2007, p. A8, en ligne : <http://technaute.cyberpresse.ca/nouvelles/internet/200705/16/01-11149-site-web-diffamatoire-six-eleves-suspendus.php> (site consulté le 12 mai 2010).

40 « Cops: Teen coerced to expose herself over Web », Msn, Associated Press, en ligne : <http://www.msnbc.msn.com/id/16047017/> (site consulté le 13 mai 2010).

e. Le harcèlement

Les sites de réseaux sociaux peuvent aussi donner lieu à du harcèlement ou à de l'intimidation. Selon l'Observatoire des droits de l'Internet de Belgique, le cyberharcèlement se définit par les éléments suivants :

1. Être **destiné à blesser** (du point de vue de l'expéditeur et/ou du destinataire).
2. Faire partie d'un **modèle répétitif** d'actions en ligne et/ou hors ligne négatives, le caractère 'répétitif' pouvant également être interprété comme l'envoi ou la consultation multiple d'un seul message déterminé.
3. Se manifester dans une relation qui est caractérisée par un **déséquilibre des rapports de forces**, se basant sur des critères de la 'vie réelle' (comme la force physique, l'âge) et/ou des critères 'relatifs aux TIC3' (comme le savoir-faire technologique, la technopuissance ou également l'anonymat ou l'adoption d'un pseudonyme).
4. Apparition dans le cadre de **groupes sociaux existants (en ligne et/ou hors ligne)**.
5. Être orienté **vers un individu**[41].

Plusieurs des fonctions des réseaux sociaux peuvent être détournées afin de harceler d'autres personnes. Par exemple, les fonctions de messageries peuvent être utilisées afin d'interagir directement avec une personne. L'affichage d'informations peut aussi servir à harceler une autre personne.

En Angleterre, Keeley Houghton, une jeune femme de 18 ans, a été condamnée pour harcèlement parce qu'elle avait menacé de mort une autre jeune femme sur sa page Facebook. Le juge l'a condamné à trois mois de détention dans une institution pour jeunes délinquants. Il s'agirait du premier cas britannique d'emprisonnement pour cyberintimidation[42].

La révélation de renseignements personnels (identité, adresse personnelle, numéro de téléphone, école fréquentée) peut donner lieu à du harcèlement, à l'envoi de menaces, de pourriels (messages importuns et non sollicités, généralement publicitaires), de contenus pornographiques ou sexuels et même à des rencontres dans la vie réelle avec des personnes qui ne sont pas telles qu'elles se décrivent.

Ainsi, le *European Network and Information Security Agency* (ENISA, une agence de l'Union européenne) révèle dans un texte de 2007 que les usagers ne sont souvent pas au courant de l'importance de l'audience ayant accès au contenu de leurs informations.

---

41 En ligne: <http://www.internet-observatory.be/internet_observatory/home_fr.htm>. Voir aussi : STALKING RESSOURCE CENTER' Social Networking Sites : A Bonanza for Stalkers ?, en ligne: <http://www.ncvc.org/ src/main.aspx?dbID=DB_ SocialNetworkingSites932 >.

42 Luke SALKELD, « Facebook Bully Jailed : Death Threat Girl, 18, is First Person Put Behind the Bars for Vicious Internet Campaign », *Mail Online*, 21 août 2009, en ligne: <http://www.dailymail.co.uk/ news/article-1208147/First-cyberbully-jailed-Facebook-death-threats.html> (site consulté le 12 mai 2010).

Ainsi, le sentiment d'intimité engendré par le fait d'être un « ami » numérique avec d'autres personnes peut mener à des révélations inappropriées ou dommageables. Par exemple, un bref survol des réseaux sociaux démontre que plusieurs personnes répondent publiquement à des questions telles que; avez-vous déjà volé de l'argent d'un ami ? Avez-vous déjà été infidèle en relation de couple ? Avez-vous déjà bu une bouteille d'alcool par vous-mêmes ? Les réponses à ces questions apparaissent avec une image reconnaissable de la personne qui répond au sondage[43].

f. L'utilisation décontextualisée des renseignements personnels

Les possibilités d'utilisation des renseignements personnels dans un contexte différent de celui dans lequel ils ont été initialement partagés constituent un autre ensemble de risques. Sur les sites de réseautage social, les gens révèlent beaucoup d'information sur eux-mêmes, mais ne sont pas toujours conscients de l'identité de ceux qui peuvent avoir accès à leur profil et des options de confidentialité disponibles.

Les informations personnelles dévoilées sur un site de réseautage social peuvent être utilisées de plusieurs façons. Par exemple, des entreprises peuvent se servir des informations pour sonder le marché, des prédateurs sexuels peuvent trouver des victimes potentielles en recherchant des profils vulnérables ou des employeurs éventuels peuvent surfer sur les espaces personnels pour en apprendre plus sur des candidats avant de les engager[44].

Par exemple, une adolescente britannique a été congédiée pour avoir exprimé sur Facebook qu'elle trouvait son emploi ennuyant. Alors que l'employeur le perçoit comme une rupture du lien de confiance, la jeune femme affirme qu'elle n'était pas malheureuse au travail et soutient qu'elle n'avait pas nommé l'employeur[45].

g. Les rencontres hors ligne avec des étrangers

Il est possible de vouloir prendre contact dans la réalité avec une personne faisant partie de notre réseau social virtuel. Ces rencontres peuvent être risquées puisqu'il est facile pour un individu de se faire passer pour quelqu'un d'autre sur ces sites. Un tel rendez-vous peut aboutir à la propagation de menaces ou à la commission d'actes de violence tels des agressions sexuelles.

---

43 EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, « Security Issues and Recommendations for Online Social Networks », *ENISA Position Paper* n° *1,* octobre 2007, en ligne : <http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks> (site consulté le 12 mai 2010).

44 Samantha L. MILLIER, « The Facebook Frontier : Responding to the Changing Face of Privacy on the Internet », (2008-2009) 97 *Kentucky L. J.*, 541-564, 544.

45 « Sacked For Calling Job Boring On Facebook », *Sky News*, 27 février 2009, en ligne: <http://news.sky.com/skynews/Home/UK-News/Facebook-Sacking-Kimberley-Swann-From-Clacton-Essex-Sacked-For-Calling-Job-Boring/Article/200902415230508> (site consulté le 4 février 2011).

Pensons à l'affaire où un homme, un dénommé Aubut, s'est fait passer pour une femme de 22 ans et est entré en contact avec une adolescente de 15 ans, à qui il a proposé de travailler dans le domaine de la pornographie. L'adolescente devait d'abord rencontrer « son patron », qui était en fait lui-même. Cette rencontre a éventuellement eût lieu et Monsieur Aubut a alors eu des relations sexuelles complètes avec l'adolescente. Il a été inculpé pour leurre (article 172.1 du *Code criminel*) et contact sexuel (article 151 du *Code criminel*)[46].

Selon une étude[47], plus du tiers des jeunes, soit 37 % des 13-17 ans, ont accepté une « demande d'ami » de quelqu'un qu'ils ne connaissaient pas. Et une autre étude, cette fois du *National Center for Exploited and Missing Children*, affirme que les 15 à 18 ans sont le groupe d'âge le plus sollicité[48].

De plus, les sites de réseautage social se révèlent être parfois des lieux dangereux permettant aux prédateurs de rencontrer des enfants. Règle générale, le scénario est le suivant : un individu se joint à un site de réseautage social afin de trouver un enfant qu'il croit vulnérable; puis il gagne sa confiance en lui parlant de sujets qui l'intéressent; enfin suivent des échanges par courriel, par téléphone, puis finalement une rencontre face à face.

Questions à vérifier

- *Le site offre-t-il la possibilité de communiquer de façon privée ?*
- *Le participant est-il amené à dévoiler des renseignements personnels sur lui-même ou sur une autre personne ?*

h. Les contenus ne convenant pas aux enfants

Il est possible de trouver des images à caractère pornographique dans les espaces personnels des gens qui sont inscrits à des sites de réseautage social. Ce contenu, quoique généralement interdit dans les conditions d'utilisation de ces sites, peut ne pas convenir aux enfants. Lorsqu'un tel contenu est dénoncé, les administrateurs du site retirent habituellement le contenu en question ou encore ferment le compte de la personne fautive. Il est tout de même possible pour un enfant de voir par inadvertance un contenu non approprié pour son âge.

---

46 *R.* c. *Aubut*, 2008 QCCQ 7722 (CanLII).

47 Microsoft, « Un sondage révèle que la sécurité en ligne est l'une des principales préoccupations des jeunes Canadiens, mais qu'ils sont nombreux à adopter un comportement à risque », 25 février 2009, en ligne : <http://nouvelles.microsoft.ca/communiques_de_presse_grand_public/archive/2009/02/25/un-sondage-r-233-v-232-le-que-la-s-233-curit-233-en-ligne-est-l-une-des-principales-pr-233-occupations-des-jeunes-canadiens-mais-qu-ils-sont-nombreux-224-adopter-un-comportement-224-risque.aspx> (site consulté le 12 mai 2010).

48 Susan HANLEY DUNCAN, « MySpace is Also Their Space : Ideas for Keeping Children Safe from Sexual Predators on Social Networking Sites », *Kentucky Law Journal*, 96, 2008, p. 539, citant YOUTH INTERNET SAFERTY TASK FORCE, *Official Report,* 20 décembre 2006, en ligne : <http://vapta.org/ Health/Report YISTFfinal.pdf>.

Certains sites de réseautage social vont proposer un service exclusivement pour les adultes où le contenu à caractère pornographique est autorisé. Il est alors plus facile d'éviter de naviguer sur ces sites lorsque c'est notre intention.

Questions à vérifier

- *Quelles sont les précautions prises pour limiter l'accès à des documents qui ne sont pas appropriés pour les enfants ?*
- *Quel est le public visé ? Le contenu est-il approprié pour ce public ?*

i. Le risque de falsification d'identité

Il est possible de contourner les conditions d'utilisation des sites de réseautage social, notamment en vue de générer des faux profils. Les usagers ont un sentiment d'anonymat et d'impunité pour leurs actions « virtuelles ». De plus, il est difficile d'identifier les coupables.

Un utilisateur peut créer un faux profil afin de nuire à une autre personne ou de faire une blague. Par exemple, un candidat à un poste pourrait créer un profil défavorable au nom d'un compétiteur afin de miner ses chances et ainsi augmenter les siennes. Au Royaume-Uni, Grant Raphael a été reconnu coupable d'atteintes à la vie privée et de diffamation pour avoir publié de fausses informations sur un ancien collègue d'école, Mathew Firsht, via un faux profil (notamment sur son orientation sexuelle et ses opinions politiques, ainsi que des allégations concernant des dettes de sa compagnie, mettant en doute la fiabilité de celle-ci). M. Firsht a obtenu 22 000 livres sterling (40 000 $ CAD) de dommages, et sa compagnie 5 000 livres sterling (9 000 $ CAD)[49].

Pour faire la promotion d'une biographie non autorisée sur Guy Laliberté, l'auteur de la biographie et son éditeur ont mis en ligne une page MySpace au nom de Monsieur Laliberté, usurpant ainsi son identité et trompant les internautes. La Cour supérieure conclut à la violation de la vie privée du demandeur Laliberté et indique qu'« il s'agit clairement d'une ingérence dans la sphère privée de la personne. Il n'y a aucune légitimité à emprunter l'identité d'une personne pour laisser croire qu'il est le destinataire de la correspondance qui lui est adressée et qu'il est l'auteur des réponses qui y sont données »[50]. Le 22 décembre 2009, la juge Laberge prononce une injonction interlocutoire pour obliger le biographe à désactiver les sites Web en question et à inscrire sur toute publicité du livre par Internet qu'il s'agit d'une biographie non autorisée.

---

49 « Payout for False Facebook Profile », *BBC News*, 24 juillet 2008, en ligne : <http://news. bbc.co.uk/2/hi/ 7523128.stm> (site consulté le 12 mai 2010).

50 *Laliberté* c. *Transit Éditeur inc.*, 2009 QCCS 6177 (CanLII), par. 30.

j. Le risque de vol d'information personnelle, vol d'identité, sollicitation indésirable

Sur les sites de réseautage social, les personnes révèlent beaucoup d'information sur elles-mêmes, mais ne sont pas très conscientes de qui peut avoir accès à leur profil et des options de confidentialité disponibles.

Certains ont dénoncé la facilité d'accès aux profils personnels sur les sites de réseautage social et les possibilités de référencement[51] (*data mining* et *spidering*) et d'hameçonnage[52] (*phishing*) qui sont susceptibles de survenir.

Les questions usuelles de sécurité (nom, adresse, nom de son animal de compagnie, nom de jeune fille de sa mère...) peuvent souvent trouver réponse dans une page Facebook. Or malgré les consignes de sécurité, plusieurs personnes utilisent des informations personnelles pour générer leurs mots de passe, ce qui facilite le travail de fraudeurs.

k. L'utilisation des sites de réseautage à des fins judiciaires ou disciplinaires

Les informations consignées dans les environnements des réseaux sociaux sont susceptibles d'être utilisées dans le cadre de procédures devant les tribunaux ou devant des instances disciplinaires[53].

L'usager aura beau configurer son profil de façon à ne réserver qu'à des « amis » triés sur le volet l'accès à certaines informations, il lui sera impossible d'exclure le droit d'autres entités d'avoir accès à ces informations, notamment dans le cadre de litiges devant les tribunaux.

Le pouvoir des tribunaux d'ordonner la production de contenus, même privés, sur les réseaux sociaux constitue le principal risque de régulation découlant des activités des réseaux sociaux. Ainsi, les photos et propos publiés sur les sites de réseautage social sont souvent utilisés en preuve pour constater des méfaits, que ce soit la consommation d'alcool par des mineurs, l'identification de manifestants ou la brutalité policière. Par exemple, ces informations sont régulièrement mises en preuve pour trancher l'attribution de la garde des enfants.

---

51 WIKIPÉDIA, « Robot d'indexation », en ligne : < fr.wikipedia.org/wiki/Robot_d%27indexation> (site consulté le 12 mai 2010).

52 WIKIPÉDIA, « Hameçonnage », en ligne : <fr.wikipedia.org/wiki/Hameconnage> (site consulté le 12 mai 2010).

53 Nicolas W. VERMEYS, « L'admissibilité en preuve de contenus issus de sites de réseaux sociaux », *Repères*, Juillet 2010, EYB2010REP962; Pamela D. PENGELLEY, *Fessing Up to Facebook : Recent Trends in the Use of Social Network Websites for Insurance Litigation,* March 3, 2009, en ligne : <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1352670>.

Les sites sont également utilisés pour justifier des mesures disciplinaires, notamment envers des élèves aux propos incendiaires envers leurs professeurs ou les membres de direction, ou envers des employés aux « cybercomportements » discutables. Par exemple, six élèves d'une école secondaire de Pointe-Claire ont écopé de suspension de deux à quatre jours pour avoir participé à un forum de discussion diffamatoire sur Facebook. Une vingtaine d'enseignants ont été visés par leur propos : entre autres choses, certains ont été accusés de pédophilie[54].

l. La persistance de l'information

La possibilité pour l'usager de supprimer complètement son compte peut poser des difficultés. Ainsi, pendant les premières années de mise en service, il était pratiquement impossible de supprimer son compte Facebook. En effet, seule la désactivation était possible jusqu'à récemment. Il est maintenant possible de supprimer complètement son compte : les informations ne pourront plus être retrouvées si la personne décide de s'ouvrir un compte de nouveau. Par contre, même en supprimant son profil, il est impossible de savoir si Facebook conserve effectivement ces données sur ses serveurs, et si oui, à quelles fins, et pour combien de temps. À ce sujet, une étude de l'Université de Cambridge a montré que les photos supprimées sur des sites de réseautage social pouvaient demeurer en ligne jusqu'à plus de 30 jours après leur suppression. C'est le cas de sept des trente sites testés, dont Facebook[55].

3. Comment évaluer ces risques ?

a. Les comportements et les caractéristiques des usagers

Dans les réseaux sociaux, plusieurs risques découlent principalement des comportements adoptés par les internautes. On se retrouve donc avec une multitude de centres de décision tous en mesure de diffuser des informations à partir de leurs perspectives. Ce rôle accru de l'amateur dans des situations autrefois dominées par des professionnels tend à brouiller les frontières entre producteur et consommateur, ce qui dramatise la question des statuts et responsabilités respectives des uns et des autres[56].

Les caractéristiques de l'usager, en particulier l'âge et le degré de maturité, influencent l'ampleur des risques. Des enfants peuvent écouter ou visionner des contenus illicites ou non appropriés pour eux. Un site qui serait destiné en priorité aux enfants, par exemple, devrait éviter de publier du contenu qui pourrait être choquant pour eux. Il est

---

54 Tristan PÉLOQUIN, « Site Web diffamatoire: six élèves suspendus », *La Presse*, 16 mai 2007, en ligne : <http://technaute.cyberpresse.ca/nouvelles/internet/200705/16/01-11149-site-web-diffamatoire-six-eleves-suspendus.php> (site consulté le 12 mai 2010).

55 « Websites Keeping Deleted Photos », *BBC News UK*, 21 mai 2009, en ligne : <http://news.bbc.co.uk/2/hi/ uk_news/8060407.stm> (site consulté le 12 mai 2010).

56 Pierre-Yves GAUTIER, « Le contenu généré par l'utilisateur », *LÉGICOM*, n° 41, 2008/1, p. 1-7.

à noter que plusieurs sites de réseautage social exigent un âge minimum pour accéder au site, que ce soit treize ans ou encore dix-huit ans.

> ***Questions à vérifier***
> - *Quel est le public visé par le site de réseautage social ?*
> - *Est-ce que l'on retrouve du contenu qui pourrait être inapproprié pour le public visé ?*

b. Les services offerts par le site de réseautage social

Le niveau de risque sur un site de réseautage social variera en fonction des services offerts sur le site. Un site proposant simplement un moyen de mettre en relation des personnes présentera nécessairement moins de risque qu'un autre offrant des fonctions de partage de contenu, de blogue et de messagerie instantanée. Dans ce dernier cas, des problèmes de droit d'auteur ou de diffamation sont plus susceptibles de survenir.

> ***Question à vérifier***
> - *Est-ce qu'il y a présence de sons, d'images ou de vidéos sur le site de réseautage social ? Si oui, est-ce que l'usager détient les autorisations nécessaires pour les utiliser ?*

c. La présence de surveillance sur le site

Il est possible qu'un site exerce une vérification de son contenu, généralement au hasard. Lorsqu'un contenu inapproprié est découvert, les administrateurs doivent prendre des moyens pour l'enlever. Par contre, les tribunaux québécois n'ont pas encore tranché la question à savoir si un site qui exerce une vérification aléatoire de son contenu peut en être tenu responsable. Il convient donc de faire preuve de prudence en optant pour cette façon de faire, en particulier s'il est impossible de vérifier tout le contenu du site vu son ampleur.

> ***Questions à vérifier***
> - *Les administrateurs du site exercent-ils une vérification sur le contenu publié ?*
> - *Quelles sont les conséquences lorsqu'une personne publie du matériel inapproprié ?*

d. La présence d'un moyen de dénoncer le contenu inapproprié

Certains sites proposent aux usagers un moyen de dénoncer un espace personnel au contenu inapproprié. Cette façon de faire est généralement efficace puisque les administrateurs du site seuls ne peuvent pas surveiller tout le contenu hébergé. De plus, une telle procédure incite les usagers à ne pas publier de matériel offensant puisqu'ils ont plus de risques de se faire dénoncer.

Question à vérifier
- *Est-ce qu'il y a une procédure de vérification par les tiers du contenu sur le site ? Si oui, cette procédure est-elle facile d'utilisation ?*

4. Quelles sont les précautions à prendre ?

La grande liberté dont dispose l'usager dans les sites de réseaux sociaux fait en sorte qu'il lui incombe de prendre les précautions qui sont appropriées aux risques qu'il accepte de courir dans ces environnements.

a. Éviter de mettre en ligne des renseignements personnels

Lors de l'inscription sur un site de réseautage social, il faut éviter de donner des renseignements personnels comme son nom et son prénom, son adresse, ou sa date de naissance, de fournir son numéro de carte d'assurance-maladie, d'assurance sociale, ou encore de carte bancaire. Des renseignements à première vue anodins, comme nos endroits préférés de sortie, peuvent aussi être utilisés à mauvais escient.

De plus, il faut faire attention aux messages publiés dans son profil ou dans celui de ses contacts puisque des informations personnelles peuvent s'y glisser. Il peut être avisé de naviguer régulièrement sur les profils de ses différents amis pour vérifier qu'aucun renseignement nous concernant n'y est inscrit.

Il faut aussi s'abstenir de publier sur un tel site des propos ou des photos susceptibles de nuire à des proches, ainsi que des propos mensongers ou diffamants, et ce, même si les paramètres de confidentialité sont élevés.

Il peut être également utile de vérifier qu'il n'y a rien d'indésirable ou de mensonger à son sujet sur le Web (ou au sujet d'un homonyme), par exemple en étant à l'affût des photos compromettantes qui pourraient être diffusées par des amis ou des connaissances. En effet, toute information qui se retrouve sur un site de réseautage social est susceptible d'être lue par le grand public.

b. Mettre en place un haut degré de protection de notre profil et éviter le contact avec des inconnus

Les sites de réseautage social mettent habituellement à la disposition des utilisateurs une page où il est possible de changer les paramètres de sécurité de son profil. Les usagers peuvent donc afficher leur profil comme étant privé, ce qui permet seulement à leurs amis de le voir, ou encore ils peuvent bloquer certaines fonctions comme la possibilité de laisser des commentaires ou d'utiliser la messagerie instantanée.

Il est important, pour plus de sécurité, de choisir un site de réseautage qui offre la possibilité d'ajuster ces paramètres. De plus, lorsque cette fonction est disponible, les

utilisateurs du service devraient appliquer le plus haut degré de protection possible à leur profil.

Pour une plus grande sécurité, refuser d'entrer en contact avec des gens que l'on ne connaît pas dans la « vraie» vie est une précaution fondamentale, mais qui n'est pas toujours infaillible.

c. Mettre en ligne une procédure de dénonciation

Une procédure de vérification du site par les utilisateurs peut être très utile pour contrôler le contenu d'un site de réseautage social. Ainsi, le site peut inviter les usagers, par une méthode facile, à dénoncer un contenu illicite. En plus de disposer d'un plus grand nombre de vérificateurs, puisque tous les visiteurs peuvent dénoncer un profil, cette méthode n'engagera généralement pas la responsabilité du site, à moins qu'il ait été averti du caractère illicite d'un contenu et qu'il ne l'ait pas promptement retiré (art. 22 de *Loi concernant le cadre juridique des technologies de l'information*).

d. Informer les participants des risques liés à l'usage des sites de réseautage social

L'usager doit s'informer des dangers liés à l'utilisation d'un site de réseau social. Ces informations devraient d'ailleurs être disponibles sur le site pour consultation par les usagers.

D'ailleurs, le site MySpace contient des mises en garde destinées précisément aux adolescents[57]. On tente de faire prendre conscience aux usagers des risques reliés aux réseaux sociaux.

- **N'oublie pas que ton profil et les forums MySpace sont publics.** Ne publie aucun contenu que tu ne souhaites pas voir exposé au monde entier (numéro de téléphone, adresse, pseudo de messagerie instantanée, lieux de sortie, etc.). Évite de publier des informations qui pourraient permettre aux inconnus de te trouver facilement, par exemple les lieux que tu fréquentes au quotidien ou une photo de toi en face de ton lieu de travail ou de ton école.

- **Les gens ne sont pas toujours tels qu'ils se décrivent.** Sois vigilant lorsque tu ajoutes des inconnus à ta liste d'amis. Il est certes amusant de se faire de nouveaux amis via MySpace dans le monde entier, mais tu dois impérativement éviter de rencontrer en personne des gens que tu ne connais pas très bien. Si tu dois absolument rencontrer quelqu'un, le rendez-vous doit être organisé dans un lieu public, en présence d'amis ou d'un adulte de confiance.

- **Les cas de harcèlement, les propos d'incitation à la haine et autres contenus inappropriés doivent être signalés.** Si tu estimes que quelqu'un a un comportement déplacé, signale-le à MySpace ou aux autorités judiciaires.

---

57 MySpace, « Conseils et paramètres de sécurité MySpace », en ligne : <http://www.myspace.com/international#!/help/safety/tips> (site consulté le 13 mai 2010).

- **Ne publie aucun contenu qui pourrait plus tard te mettre dans une situation embarrassante.** On s'imagine facilement que seuls nos amis consultent notre page MySpace, mais en réalité tout le monde peut y accéder. Réfléchis-y à deux fois avant de publier une photo ou des informations que tu ne veux pas exposer à tes parents, aux employeurs potentiels, aux établissements scolaires ou à ton patron!

- **Ne prétends pas avoir plus ou moins de 18 ans si ce n'est pas le cas.** Si le service client de MySpace découvre que tu as moins de 13 ans alors que tu prétends être plus âgé, ton profil sera supprimé. De même, si nous découvrons que tu as plus de 18 ans alors que tu prétends être plus jeune pour pouvoir contacter les utilisateurs mineurs, ton profil sera également supprimé.

Le besoin d'information est tout particulièrement grand lorsque les participants sont des enfants. Des mises en garde concernant les prédateurs sexuels en ligne, la divulgation de renseignements personnels ou encore les rencontres hors ligne avec des inconnus peuvent s'avérer très utiles. Il faut également inciter les enfants à utiliser des paramètres de sécurité élevés et être à l'affût de leurs changements de comportement.

Afin d'assurer une plus grande protection aux enfants, diverses mesures ont été mises en place dans plusieurs états. Ainsi, suite à l'enlèvement, au viol et au meurtre de l'adolescente Ashleigh Hall, les autorités britanniques ont demandé à Facebook de doter son site d'un bouton d'alerte afin de permettre aux jeunes qui se sentent en danger d'obtenir l'aide immédiate de la police par un simple clic de souris. Dans ce cas, l'homme de 32 ans qui a tué l'adolescente s'était fait passer pour un jeune homme de 16 ans sur Facebook afin d'entrer en relation avec la jeune fille et par la suite de prévoir une rencontre en personne[58].

En Ontario, pour que les enfants puissent davantage se protéger lorsqu'ils naviguent sur Internet, le gouvernement a modifié le cursus scolaire des écoles primaires afin d'intégrer, depuis l'automne 2010, des cours sur la sécurité en ligne.[59].

B. Les sites de partage de contenu

1. Qu'est-ce qu'un site de partage de contenu ?

Un site de partage de contenu est un site Web où les visiteurs ont la possibilité de mettre en ligne des fichiers, que ce soit des vidéos, des chansons, des livres, etc. En général, ces sites utiliseront la lecture en transit pour diffuser le contenu. Pour visionner

---

58 « Londres veut un « bouton d'alerte » sur les pages Facebook », Canoë, 11 mars 2010, en ligne : <http://www2.canoe.com/techno/nouvelles/archives/2010/03/20100311-135416.html> (site consulté le 12 mai 2010).

59 « Ontario Adds Internet Safety to Elementary Curriculum », Canadian Press, *The Globe and Mail*, 10 mars 2010, en ligne : <http://www.theglobeandmail.com/news/national/ontario-adds-internet-safety-to-elementary-curriculum/article1496713/>.

un film, par exemple, il suffit d'aller sur un site Internet qui offre ce service, de sélectionner le film, et de l'écouter, sans besoin de l'enregistrer sur un disque dur.

La lecture en transit (*streaming*) est une méthode de téléchargement de fichiers audio ou vidéo qui permet leur lecture en temps réel, c'est-à-dire dès le début de la réception du fichier, sans avoir à attendre qu'il soit copié au complet sur l'ordinateur récepteur. Le transfert de données se fait sous forme de flux régulier et continu. La lecture en transit permet donc de diffuser des contenus multimédias sur Internet, à la demande ou en temps réel, et ce sans solliciter l'espace du disque dur de l'utilisateur.

Les applications de cette technique sont nombreuses : radio et télévision sur Internet, vidéo à la demande, informations audiovisuelles en continu… Pour les compagnies de disques, il s'agit là d'une alternative aux fichiers MP3. Elles peuvent faire valoir leurs produits sans risquer de les faire copier puisqu'il n'y a pas, en principe, de copie durable du fichier transféré.

Les sites les plus connus de partage de contenu sont sans aucun doute YouTube (http://www.youtube.com/) et Dailymotion (http://www.dailymotion.com/). Les visiteurs de tels sites peuvent y publier des films, des vidéoclips, des émissions, etc. Ils peuvent aussi visionner le contenu que d'autres visiteurs ont publié. Les sites de réseaux sociaux sont également utilisés pour partager du contenu puisque certains hébergeurs d'espaces personnels offrent, par exemple, la possibilité aux membres de mettre en ligne leur musique préférée.

Les sites de partage de contenu offrent en général la possibilité aux visiteurs de laisser des commentaires suite au visionnement de la vidéo ou à l'écoute de la chanson. Il est aussi possible d'évaluer le document en lui accordant une note, généralement sur cinq (exemple : quatre étoiles sur cinq). Ce système de notation permet de faire une recherche sur le site par rapport au contenu le mieux coté.

Ces sites sont très intéressants pour ceux qui désirent publier du contenu puisque le service est habituellement gratuit. Les coûts de bande passante seront moindres en publiant des vidéos sur YouTube, par exemple, au lieu de les mettre directement sur une page Web personnelle. Il est possible par la suite d'incorporer la vidéo (*embedding*) directement sur le site personnel. De plus, la publication ne demande aucune connaissance particulière en informatique.

En 2011, Youtube était le troisième site le plus fréquenté au monde – après Google et Facebook, respectivement en première et seconde place[60]. Le géant du partage de contenu limite les fichiers audiovisuels déposés sur son site à 10 minutes et à un maximum de 2 Go. Avant le 1er juillet 2009, le poids était limité à 1 Go, mais YouTube a doublé le maximum pour accommoder le HD, sans toutefois modifier la limite de 10

---

60 « Top Sites », Alexa.com – the Web Information Company, en ligne : <http://www.alexa.com/ topsites> (site consulté le 7 septembre 2010).

minutes[61]. Ces limitations, ainsi que le slogan « Broadcast Yourself », montrent la volonté de YouTube de miser sur les vidéos amateurs et d'éviter le plus possible la diffusion de contenus protégés par le droit d'auteur. Il existe d'autres sites de partage tels RapidShare.com, Flickr.com, Tagged.com, Revver.com, Blip.tv et Vuze.com.

a. Qui fait quoi ?

i) Les usagers

La personne qui consulte un site de partage de contenu peut jouer deux rôles.

Il peut être ***visiteur***; il peut naviguer sur le site pour chercher une vidéo ou un film. Une fois le contenu téléchargé ou visionné, il est souvent amené à l'évaluer et à le commenter.

Il peut également être un ***participant.*** Il mettra alors des éléments (vidéos, images, films) sur le site de partage de contenus. Dans le cadre de sites de poste-à-poste, il participera activement, comme client et comme serveur.

ii) Les hébergeurs

Les hébergeurs créent l'architecture informatique permettant à l'utilisateur de téléverser et ensuite de visionner le contenu. Ils mettent en place des mécanismes automatiques qui convertissent le contenu dans un format uniforme, lisible par tous les visiteurs. Ce sont aussi eux qui décident de garder ou de retirer un contenu lorsque celui-ci fait l'objet d'un blâme (flag).

Les hébergeurs doivent agir rapidement lorsqu'une vidéo inappropriée diffusée sur leur site leur est signalée, mais il est difficile de les en tenir responsables lorsqu'ils n'ont pas connaissance des contenus illicites. La tâche de visionnement préalable semble impensable pour un site comme YouTube, considérant la quantité phénoménale de vidéos mises en ligne, estimée en mai 2011 à 48 heures de matériel par minute[62].

iii) Les « communautés »

On désigne par « communauté » l'ensemble des usagers qui consultent, évaluent et commentent le contenu d'un site. Elle occupe une place importante dans le fonctionnement des sites de partage de contenu. Le nombre de consultations, la note globale et le nombre de commentaires déterminent ensuite la présentation du contenu

---

61 Ryan JUNEE, « Upload Sizes Doubles + DH Tips », Youtube Canada's Official Blog, 1er juillet 2009, en ligne : <http://youtube-global.blogspot.com/2009/07/upload-size-doubles-hd-tips_8074.html> (site consulté le 31 mai 2010).

62 The Official YouTube Blog, « Thanks, YouTube community, for two BIG gifts on our sixth birthday!», YouTube, 25 mai 2011, en ligne: <http://youtube-global.blogspot.com/2011/05/thanks-youtube-community-for-two-big.html> (site consulté le 1er juin 2010).

sur le site. Par exemple, dans une recherche effectuée sur YouTube, les « meilleures » vidéos selon ces critères apparaîtront en premier sur le site.

b. Utilisation des sites de partage de contenu en éducation

Les sites de partage de contenu permettent aux enseignants d'offrir des cours en ligne. Certains d'entre eux mettent des vidéos en ligne pour résumer leur cours et ainsi aider leurs élèves dans leur étude. De plus, beaucoup de projets scolaires réalisés par les élèves – que ce soit dans le cadre de cours de technologie ou non – et des vidéos éducationnelles se retrouvent sur YouTube[63]. Règle générale, les vidéos sur YouTube sont publiques, mais il est possible de les rendre privées et cela peut être un élément intéressant pour dynamiser l'étude et les devoirs[64].

Il existe des sites Web basés sur la même formule que YouTube, mais qui sont spécifiques au monde de l'éducation. C'est le cas notamment de TeacherTube.com et de SchoolTube.com. Le premier vise la coopération entre enseignants. Ces derniers peuvent y publier des vidéos afin d'illustrer leur façon d'enseigner[65]. Quant à SchoolTube.com, il s'agit d'un site où l'on retrouve du contenu créé par les élèves[66]. C'est un site plus sécuritaire que YouTube; une personne voulant utiliser le site scolaire doit obligatoirement se créer un compte. Un représentant de SchoolTube s'assurera ensuite que l'école existe réellement. Par la suite, les vidéos soumises par les élèves doivent être approuvées par un enseignant avant d'être publiées et celui-ci peut décider qui y aura accès[67]. En plus de présenter des projets scolaires sous forme de vidéos, les élèves peuvent participer à des concours organisés par le site[68].

2. Quels sont les risques associés aux sites de partage de contenu ?

Les risques associés aux sites de partage de contenu sont semblables à ceux reliés aux sites de réseaux sociaux. En effet, plusieurs sites de réseaux sociaux offrent également

---

63 Sara CARDINE, « Is Education Ready For YouTube ? », Converge.com, en ligne : <http://www. convergemag.com/edtech/Is-Education-Ready-For-YouTube.html> (site consulté le 3 juin 2010).

64 « Premiers pas: Vidéos privées (procédure de partage) », YouTube, en ligne : <http://www. google.com/support/youtube/bin/answer.py?hl=fr&answer=157177> (site consulté le 3 juin 2010).

65 Sara CARDINE, « Is Education Ready For YouTube ? », Converge.com, 21 juillet 2008, en ligne : <http://www. convergemag.com/edtech/Is-Education-Ready-For-YouTube.html> (site consulté le 3 juin 2010).

66 Sara CARDINE, « Is Education Ready For YouTube ? », Converge.com, 21 juillet 2008, en ligne : <http://www. convergemag.com/edtech/Is-Education-Ready-For-YouTube.html> (site consulté le 3 juin 2010).

67 « SCHOOLTUBE : Free Web Based, Education Focused Video Sharing Site», DE Tools of the Trade, en ligne : <http://www.detools.ca/?p=2959> (site consulté le 3 juin 2010).

68 « SCHOOLTUBE : Teacher Approved Education Videos », SchoolTools, 17 juillet 2009, en ligne : <http://www.schooltoolsblog.com/schooltube-teacher-approved-education-videos/> (site consulté le 3 juin 2010).

un service de partage de contenu avec ses contacts, par exemple de musique ou encore de films.

a. L'utilisation non autorisée de l'image et de renseignements personnels

Du contenu de nature personnelle ou relevant du cercle intime d'une personne peut se retrouver sur des sites de partage de contenu, tels des vidéos de fêtes ou encore de sorties entre amis. Ces vidéos peuvent brimer le droit à l'image de quelqu'un s'il est possible d'identifier la personne filmée. Il n'est même pas nécessaire d'utiliser l'image réelle de cette personne pour transgresser ses droits. En effet, l'utilisation d'un sosie dans une vidéo et la mention du nom de la personne imitée peuvent suffire à violer le droit à l'image.

Il faut donc s'assurer, avant de publier une vidéo sur Internet, d'avoir les autorisations nécessaires des personnes qui s'y retrouvent, ou qui y sont représentées. Le même raisonnement s'applique pour les autres types de contenus, par exemple pour les images qui pourraient être mises en ligne.

De plus, puisque les sites de partage de contenu demandent souvent d'inscrire une adresse de courrier électronique pour pouvoir, par exemple, publier un commentaire, il est possible que ce renseignement personnel soit utilisé pour une autre finalité, par exemple pour une liste de diffusion de pourriels. Il est aussi difficile de connaître la persistance des données personnelles et qui sont les tiers ayant accès à ces informations.

Questions à vérifier

- *Est-ce que le contenu visionné contient des images de personnes identifiables ?*
- *Est-ce que l'auteur du contenu détient les autorisations nécessaires pour le publier ?*
- *Est-ce que le site demande l'inscription d'une adresse de courriel ? Est-ce que l'adresse est diffusée sur le site ?*

b. La présence de contenu illicite, illégal ou ne convenant pas aux enfants

Les populaires sites de partage de contenus sont des espaces de choix pour partager des idées et des opinions avec un grand nombre de personnes. Toutefois, ils peuvent devenir des espaces de diffusion de contenus contraires à la loi ou ne convenant pas aux enfants. Les comportements illégaux dans la « vie réelle » le demeurent sur Internet, que ce soit les propos haineux, la diffamation, le harcèlement, les menaces ou l'intimidation.

Les actions « virtuelles » confèrent un certain sentiment d'anonymat et d'impunité. De plus, il est difficile d'identifier les coupables d'infractions. Il y a également un délai entre le moment où la vidéo est mise en ligne, le moment de son signalement comme étant inapproprié (*flagging*) et finalement le moment de son retrait. La vidéo peut donc être vue par un plus grand nombre de personnes et causer davantage de dommages.

Les sites de partage de contenu sont aussi souvent un moyen pour diffuser des vidéos d'agressions physiques, ou *happy slapping*[69]. Ces vidéos, où l'on voit une personne en train de se faire agresser par surprise et de façon tout à fait gratuite, ne sont pas encore interdites spécifiquement dans une loi au Canada. Par contre, la responsabilité des gens qui filment et publient de telles agressions peut être retenue de plusieurs autres façons. Par exemple, ils peuvent être poursuivis pour ne pas avoir porté secours à une personne en péril, obligation qui est prévue à l'article 2 de la *Charte des droits et libertés de la personne*[70]. Il est à noter que certains pays, comme la France[71], ont adopté des lois qui interdisent le *happy slapping* sous peine de se voir attribuer une amende et une peine d'emprisonnement.

Bien qu'elles ne soient pas illégales en soi, les images sexuellement explicites sont contractuellement interdites sur YouTube. Toutefois, comme la censure du site ne fonctionne pas par choix éditorial préalable, les jeunes peuvent se retrouver exposés à de la pornographie et à des contenus inappropriés. Lorsqu'un visiteur signale aux administrateurs d'un site de partage la présence de tels contenus, certains conservent ou retirent simplement le contenu, d'autres l'assortissent d'un avertissement de contenu explicite. Les enfants peuvent donc y avoir accès sur certains sites avec plus ou moins de difficulté, de façon volontaire ou non.

Dans ses conditions d'utilisation, YouTube interdit l'accès aux mineurs de moins de 13 ans et soumet les adolescents au consentement parental, mais ces conditions sont facilement contournables et il est très complexe pour un site comme YouTube de contrôler l'âge de ses utilisateurs.

Questions à vérifier

- *Quelles sont les précautions prises pour limiter l'accès à des documents qui ne sont pas appropriés pour les enfants ?*
- *Quel est le public visé ? Le contenu est-il approprié pour ce public ?*
- *Est-ce que les interventions anonymes sont permises sur le site ?*
- *Le site demande-t-il la divulgation de renseignements personnels ?*
- *Est-ce qu'il y a un mécanisme de dénonciation de propos illicites sur le site Web ?*

c. Les atteintes au droit d'auteur

Le risque le plus important sur de tels sites est sans doute celui d'utiliser du contenu protégé par le droit d'auteur. En droit d'auteur canadien, que ce soit la diffusion en transit d'une chanson, d'un vidéoclip ou d'un livre, même si une œuvre ne se retrouve jamais au complet dans la mémoire Ram de l'usager et que seules d'infimes parties s'y

---

69 INTERNATIONAL HERALD TRIBUNE. « Le côté sombre des sites de partage de contenu », dans *Canoë*, en ligne : <http://www2.canoe.com/techno/nouvelles/archives/2007/03/20070302-105546.html>, (site consulté le 1er juin 2007).

70 L.R.Q., c. C-12.

71 *Loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance*, J.O. 7 mars 2007, p. 4297, art. 44.

croisent, tour à tour, pour s'effacer lorsque la partie suivante arrive, il s'agit là, strictement parlant d'une reproduction. En dehors des cas où un détenteur des droits d'auteur propose des œuvres par ce moyen, cette technique pourrait être considérée comme une source illicite de reproduction des œuvres.

Plusieurs situations violant des droits d'auteur peuvent se produire sur les sites de partage de contenu. Par exemple, publier une vidéo dans laquelle il y a un extrait d'une autre vidéo peut conduire à des poursuites de la part de l'auteur de l'extrait[72]. De plus, mettre en ligne une vidéo de notre enfant où on utiliserait comme musique de fond une chanson qui est la propriété de quelqu'un d'autre est aussi une atteinte au droit d'auteur[73]. Il y a également la situation plus évidente où l'on met directement en ligne une œuvre qui ne nous appartient pas[74].

De plus, l'utilisation des sites pair-à-pair est très populaire chez les jeunes. En effet, selon une étude de l'Université du Hertfordshire auprès de jeunes de 14 à 24 ans, il semble que 61 % des jeunes utilisent les réseaux pair-à-pair couramment (par exemple Kazaa.com, BitTorent.com, Limewire.com, Emule.com). Chaque jeune interrogé lors de l'étude possédait environ 8 100 titres sur son ordinateur[75]. Or, cela contrevient aux lois sur le droit d'auteur étant donné que ces derniers ne paient pas de droits sur les chansons qu'ils téléchargent de cette façon.

Questions à vérifier

- *Est-ce que le contenu contient des œuvres ou parties d'œuvres qui sont protégées par la* Loi sur le droit d'auteur *?*
- *Est-ce que la personne qui diffuse l'information détient les autorisations nécessaires pour la publier ?*
- *Quels types d'œuvres sont visionnés ou écoutés ?*
- *Est-il possible de garder une copie des documents audio ou vidéo ? Internet regorge d'outils permettant d'intercepter et d'enregistrer un flux de sons ou d'images pour les divers formats utilisés.*

d. La responsabilité pour les informations diffusées

La question de savoir qui répond de l'information se retrouvant sur un site de partage de contenu reste entière. En général, les auteurs seront les premiers responsables de l'information qu'ils publient lorsqu'ils sont identifiés. Les sites eux-mêmes n'ont pas

---

72 Sur les faits et non sur le fond, voir : *Doe* v. *Geller*, 533 F. Supp.2d 996 (N.D. Cal. 2008).

73 Sur les faits et non sur le fond, voir : *Lenz* v. *Universal Music Corp.*, 2008 WL 962102 (N.D. Cal. 2008).

74 Sur les faits et non sur le fond, voir : *Viacom Intern. Inc.* v. *YouTube, Inc.*, 2008 WL 629951 (S.D. N.Y. 2008); *Jean-Yves Lafesse et autres / Dailymotion et autres*, Tribunal de grande instance de Paris, 3[e] chambre, 1[e] section, jugement du 15 avril 2008.

75 « Les 14-24 ans piratent chacun en moyenne 8 000 titres de musique », Numerama, 10 août 2009, en ligne : <http://www.numerama.com/magazine/13625-Les-14-24-ans-piratent-chacun-en-moyenne-8-000-titres-de-musique.html> (site consulté le 31 mai 2010).

d'obligation de surveiller les documents déposés par les usagers. Mais par contre, s'ils sont avertis qu'un propos ou document illicite se retrouve sur le site, ils ont l'obligation de réagir et de le retirer si c'est nécessaire[76].

> ***Questions à vérifier***
> - *Est-ce qu'il y a des mécanismes de surveillance du contenu sur le site en question ?*
> - *Les interventions anonymes sont-elles permises ?*

e. L'utilisation des sites de partage de contenu à des fins judiciaires ou disciplinaires

Sur les sites de partage de contenu, les gens diffusent des images et vidéos d'eux-mêmes et de leurs proches. Or, les vidéos publiées peuvent être utilisées en preuve et incriminer les personnes qui commettent les délits qui ont été filmés. Aussi, les vidéos pourraient éventuellement être consultées par des employeurs ou professeurs et conduire à des mesures disciplinaires. L'enjeu n'est toutefois pas aussi présent que pour les sites de réseautage social, où l'identité des personnes est plus directement dévoilée.

Par exemple, une vidéo prise sur la scène du délit par un observateur a été mise en ligne sur YouTube et a servi de preuve lors du procès[77]. Également, une vidéo diffusée sur YouTube montrant un graffitiste californien à l'œuvre sur le muret d'un viaduc a servi de preuve incriminante lors de son procès pour vandalisme[78].

Dans une affaire de 2008[79], deux adolescents ont été condamnés suite à l'enregistrement d'une vidéo. Les deux torontois planifiaient de mettre sur YouTube une vidéo « pyrotechnique » où on les verrait imbiber d'essence à briquet certaines parties de leurs vêtements et les mettre en feu. Ils ont entraîné puis forcé une copine à en faire autant, ce qui lui causé des blessures. Les vidéos en question ont été utilisées en cour pour apprécier la teneur des événements et l'absence de consentement de la jeune femme.

3. Comment évaluer ces risques ?

a. La présence d'un moyen de dénoncer le contenu inapproprié

Les sites de partage de contenu vont en général mettre à la disposition des usagers un moyen simple de dénoncer un contenu qui pourrait être considéré comme inapproprié.

---

76 *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, art. 22.

77 *R.* c. *Mason*, 2008 BCPC 147 (CanLII).

78 Andrew BLANKSTEIN, « Daredevil tagger gets nearly 4 years in prison », Los Angeles Times, 11 septembre 2009, en ligne : <http://www.latimes.com/news/local/la-me-tagger11-2009sep11,0, 4537998.story> (site consulté le 1er juin 2010).

79 *R.* v. *P. (A.P.)*, 2008 ONCJ 196 (CanLII).

Par exemple, les sites peuvent joindre à chaque vidéo un lien qui conduit à un formulaire de plainte. Ces liens se reconnaissent habituellement par la présence d'un drapeau et de la mention « *Flag this video* ». Donc, si une personne trouve une vidéo au contenu illégal, il suffit de cliquer sur le lien et de remplir le formulaire pour que la vidéo soit retirée. Certains sites par contre limitent la possibilité de faire des plaintes aux membres du site, ce qui réduit le nombre de personnes pouvant le surveiller.

Les sites peuvent également prévoir une procédure de plainte spéciale lorsqu'une personne ou une compagnie veut faire retirer un contenu dont elle détient les droits d'auteur. Cette procédure est généralement calquée sur la procédure de notification d'une infraction au droit d'auteur prévue dans le *United States Code* (17 U.S.C. § 512 (1996)).

Questions à vérifier

- *Est-ce qu'il y a une procédure disponible pour faire des plaintes concernant le contenu ? Si oui, est-ce que la procédure est simple et accessible ?*
- *Faut-il être membre du site pour réguler le contenu qui s'y trouve ?*

b. Le caractère anonyme ou non des participants

Selon le type de site, les publications anonymes peuvent être autorisées ou non. Par contre, la plupart des sites de partage ne permettent pas les soumissions anonymes ni les commentaires anonymes suite au visionnement d'un fichier. Lorsqu'il faut fournir ses coordonnées, comme son adresse de courriel, ou s'enregistrer sur le site pour y participer, les risques de comportements ou de propos inappropriés sont minimisés puisque les participants sont susceptibles d'être identifiés.

Questions à vérifier

- *Est-ce que les participants communiquent dans l'anonymat ?*
- *Est-ce que les participants utilisent des pseudonymes ?*
- *Est-ce qu'il y a des restrictions quant aux personnes pouvant publier un commentaire ?*

c. Les caractéristiques de l'usager

Les caractéristiques de l'usager, en particulier l'âge et le degré de maturité, influencent l'ampleur des risques. Des enfants pourraient écouter ou visionner des contenus illicites ou non appropriés pour eux. Un site qui serait destiné en priorité aux enfants, par exemple, devrait éviter de publier du contenu qui pourrait être choquant pour eux.

Questions à vérifier

- *Quel est le public visé par le site Internet ?*
- *Est-ce que l'on retrouve du contenu qui pourrait être inapproprié pour le public visé sur le site Internet ?*

d. La présence de modération

Comme l'ajout de commentaires est possible sur les sites de partage de contenu, les risques de dérapage sont minimisés lorsqu'il y a présence de modération. La modération peut se faire *a priori*, c'est-à-dire avant que le message soit publié sur Internet, ou encore *a posteriori*, qui signifie que le message sera immédiatement publié, avec la possibilité de le retirer si le contenu s'avère illicite.

S'il n'y a pas de modération, c'est lorsque la personne qui administre le site a connaissance du caractère illicite d'un document qu'elle a l'obligation d'agir et de le retirer[80].

Les visiteurs aussi peuvent avoir un certain contrôle sur les commentaires publiés. Pour éviter que des compagnies ou des personnes utilisent la zone de commentaires comme endroit publicitaire, certains sites permettent aux participants de supprimer des messages en les signalant comme étant du pourriel (*spam*).

Questions à vérifier
- *Est-ce que l'espace réservé au contenu est modéré ? Si oui, de quelle façon ? Cela se fait-il avant ou après la publication d'un commentaire ?*
- *Les visiteurs ont-ils la possibilité de modérer certains commentaires ?*

4. Quelles sont les précautions à prendre ?

a. Informer les participants des risques liés à l'usage des sites de partage de contenu

Il est important de sensibiliser les gens aux risques auxquels ils s'exposent en utilisant les sites de partage de contenu, que ce soit pour la préservation de leurs renseignements personnels ou pour la protection du droit d'auteur. Cette éducation doit se faire en particulier lorsque le public visé est les enfants.

b. Penser aux conséquences possibles avant la mise en ligne de matériel

Il est important de méditer sa décision avant de mettre en ligne du contenu sur un site de partage et réfléchir aux implications possibles lorsqu'on est filmé, surtout si ces images pourraient un jour se retourner contre soi (nudité, ébriété, etc).

c. S'assurer, avant de publier un fichier, que le site choisi offre un système de modération

La modération est importante pour éviter que des commentaires désobligeants se retrouvent sur un site de partage de contenu. Avant de publier du contenu sur un site, il

---

[80] *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, art. 22.

faut s'assurer qu'il offre un service de modération et vérifier si ce service est complet. Les risques de dérapage sont limités si la publication de commentaires est limitée aux seuls membres du site ou si la modération se fait *a priori*.

d. Éviter de mettre en ligne des renseignements personnels

Il ne faut pas mettre en ligne des vidéos qui pourraient nuire à ses proches ou à soi-même et vérifier que personne dans son entourage ne le fait. De plus, lors de l'inscription sur un site de partage de contenu, il est préférable de fournir le minimum d'informations personnelles.

e. Éviter de porter atteinte aux droits d'autres personnes

Il faut bien évidemment s'abstenir de publier tout matériel obscène ou haineux ou constituant une atteinte au droit d'auteur. Il faut obtenir le consentement des personnes identifiables sur les images mises en ligne, surtout si elles sont compromettantes. Il est important de respecter les lois en vigueur de son pays.

De plus, comme de nombreux sites de partage de contenu fonctionnent sur un système de « flagging », les usagers ont un rôle très important puisqu'ils peuvent dénoncer les contenus inappropriés aux administrateurs des sites de partage de contenu. On peut ainsi mettre fin à la diffusion d'images ou vidéos illicites.

f. Établir une politique d'utilisation du site de partage de contenu

Quant au site lui-même, il doit établir des règlements quant à l'utilisation de son service. Il peut, entre autres, interdire la publication de contenu à caractère sexuel, raciste, violent, etc. Il peut aussi rappeler les principes du droit d'auteur pour éviter que les usagers publient des œuvres protégées, de façon intentionnelle ou non.

Si les conditions d'utilisation ne sont pas respectées, l'administrateur de site peut se réserver le droit de supprimer le contenu ou de fermer le compte du membre.

g. Mettre sur pied un processus de vérification du contenu

Que ce soit par les utilisateurs ou par les administrateurs du site de partage de contenu, il serait prudent de mettre en place une procédure de vérification du contenu. La procédure de vérification du site par les utilisateurs peut être une bonne alternative. Il s'agit d'inviter les gens à dénoncer un contenu illicite, par une méthode facile offerte par le site. En plus de disposer d'un plus grand nombre de vérificateurs puisque tous les visiteurs peuvent dénoncer un fichier, cette méthode n'engagera pas la responsabilité du site, à moins qu'il ait été averti de l'existence d'un contenu illicite et qu'il ne l'ait pas retiré.

C. Les blogues

1. Qu'est-ce qu'un blogue ?

Un blogue, appelé également « carnet Web » ou « cybercarnet », est un site web personnel qui s'apparente à ce qu'on décrit traditionnellement comme étant un journal de bord. La personne qui anime un blogue, soit le blogueur, publie périodiquement sur son site des articles ou billets sur des sujets divers, classés du plus récent au plus ancien.

En général, un blogue sera mis à jour régulièrement par une seule personne qui en aura le contrôle, mais il est possible également que plusieurs auteurs y participent. Les lecteurs et visiteurs du blogue ont généralement la possibilité de publier un commentaire à la fin de chaque billet, de façon anonyme ou non. Il est à la discrétion du blogueur de modérer ou non les opinions publiées pour éviter que des messages illicites se retrouvent sur le site Web.

Les billets qui sont publiés sur les blogues traitent de sujets très variés, tels l'actualité, le sport, le cinéma, les voyages, ou encore les pensées personnelles du blogueur, au même titre qu'un éditorial dans un journal. Le principe est la liberté de parole, sous réserve des propos interdits par la loi, par exemple la propagande haineuse. Il est possible de faire des hyperliens vers d'autres blogues et d'autres sites Internet ou encore de faire des liens à l'intérieur du blogue lui-même, vers des billets plus anciens traitant ou non du même sujet.

Cette façon de créer un site Web se caractérise par sa grande facilité, ce qui explique en partie la popularité des blogues. En effet, aucune connaissance informatique n'est vraiment requise pour créer et mettre à jour un blogue, contrairement à un site web traditionnel[81]. La procédure de création et de mise à jour très simplifiée d'un blogue permet d'économiser beaucoup de temps. Il suffit de s'inscrire sur un site Internet gratuit qui héberge des blogues et de suivre les instructions (voir le site < http://www.blogger.com/ >, qui propose de l'hébergement de blogues gratuitement[82]). Ces sites permettent à tous de créer un blogue personnalisé avec un minimum de connaissances informatiques.

La publication d'articles sur différents sujets devient ainsi une activité à la portée de tous, peu importe l'âge, les connaissances informatiques ou le lieu de résidence. La popularité des blogues est croissante, et constitue une des sources d'information et de divertissement les plus prisées sur la toile.

---

81 En effet, la tenue d'un site Web traditionnel nécessite généralement la connaissance du langage HTML et sa mise en ligne est souvent ardue, diminuant ainsi la fréquence des mises à jour.

82 Blogger.com est la plateforme de blogues le plus populaire au monde (8e site le populaire au monde, toutes catégories confondues, 10e au Canada). Google en est propriétaire. Wordpress.com arrive au second rang (19e site le plus populaire au monde, toutes catégories confondues, 23e au Canada).

On constate également que de plus en plus, les différents types de sites Web se confondent. Par exemple, il est maintenant possible d'intégrer des vidéos puisées sur YouTube à un blogue, ou de bloguer en utilisant un site de réseautage social comme Facebook ou un site de partage de contenus comme Youtube (vidéoblogue). D'ailleurs, le site Twitter, qui s'impose sur la toile, est décrit à la fois comme un site de réseautage social et un site de « micro-blogging ». D'autre part, il existe des blogues privés et publics dont il est difficile d'évaluer la proportion relative.

a. Qui fait quoi ?

i) L'hébergeur

Tout site, forum, blogue ou image accessible sur Internet est dans les faits stocké dans un serveur. Dans le cas de blogues, un hébergeur met à la disposition des usagers ses serveurs, gratuitement ou non, pour stocker les données d'utilisateurs[83]. L'hébergeur fournit l'espace au blogueur, mais il peut aussi être responsable des propos qui y sont tenus. L'hébergeur peut aussi se voir obliger de dévoiler l'identité de blogueurs qui ont des agissements illicites.

ii) Le blogueur

Le blogueur est le créateur d'un blogue. Il peut publier sur son blogue des textes, généralement courts, des photos et des extraits musicaux.

La conception d'un tel site peut se faire grâce à une plateforme d'autopublication et d'hébergement des blogues ou bien à partir d'un logiciel de publication. La conception du blogue peut aussi se faire indirectement par le blogueur, par l'intermédiaire d'un tiers avec lequel il est lié par contrat (ex: contrat de travail, de stage ou de prestation de service).

iii) Le visiteur

Le visiteur est un acteur fondamental du blogue. En effet, chaque article publié sur un blogue peut être commenté par ceux qui le visitent et devenir le point de départ d'une discussion. C'est l'essence même d'un tel site.

Certains blogues exigent des visiteurs de s'identifier avant de pouvoir laisser un commentaire sur le site alors que d'autres sont ouverts à tous. Cela est à la discrétion du blogueur et permet une identification dans le cas de commentaires illicites.

Par exemple, pour pouvoir commenter sur les blogues des journalistes de la Presse sur Cyberpresse.ca, il faut que les visiteurs deviennent membres Cyberpresse. Cela permet un contrôle un peu plus serré sur les usagers qui commentent les blogues.

---

83 « Manuel d'utilisation », Over-blog, en ligne : <http://www.over-blog.com/manual/> (site consulté le 25 mai 2010).

iv) L'agrégateur

Un agrégateur (de l'anglais *aggregator*) est en fait un logiciel qui permet de suivre plusieurs fils de syndication simultanément.

Les fils de syndication sont très utilisés sur les blogues. En fait, chaque nouveau billet publié est transmis en quasi-temps réel aux personnes abonnées au fil du carnet, qui peuvent le lire directement dans leur agrégateur[84].

b. Utilisation des blogues en éducation

Certaines écoles ont intégré des blogues dans leurs classes[85]. Pour utiliser de tels outils dans un cadre scolaire, l'enseignant peut se créer un blogue ou demander à ses élèves de s'en créer un. Le *Réseau pour le développement des compétences de l'intégration des technologies* (RÉCIT) propose d'ailleurs trois utilisations du blogue en éducation : le blogue comme portfolio d'apprentissage, le blogue de l'enseignant et le blogue de la classe[86].

Le blogue comme portfolio d'apprentissage est un blogue géré par l'élève. Celui-ci peut y publier ses travaux et ses réflexions[87]. On peut penser qu'il pourra utiliser son blogue à des fins académiques et personnelles. Également, il faut savoir qu'un blogue est généralement public, ce qui permet entre autres aux parents de l'élève de suivre son cheminement. Le *Centre régional de documentation pédagogique d'Alsace* propose des utilisations précises des blogues en éducation[88] :

- « Blog de projet : pour accompagner un projet interdisciplinaire, la mise en place d'un spectacle, la préparation d'un voyage d'études.
- Mise en place d'ateliers, de devoirs et d'exercices en ligne.
- Présentation des productions d'écrits, le blog vu comme un atelier d'écriture ».

84 WIKIPÉDIA, « Agrégateur », en ligne : <http://fr.wikipedia.org/wiki/Agr%C3%A9gateur> (site consulté le 26 mai 2010).

85 Martine RIOUX, « Les vertus du blogue pédagogique », Infobourg, 18 décembre 2006, en ligne : <http://archives.infobourg.com/sections/editorial/editorial.php?id=11301> (site consulté le 3 mars 2012).

86 Sonia SEHILI, « Le blogue, un outil qui a du potentiel - Utilisations pédagogiques du blogue », RECIT, 17 nov. 2011, en ligne : <http://www.recit.qc.ca/article/utilisation-p%C3%A9dagogique-du-blogue> (site consulté le 3 mars 2012).

87 Sonia SEHILI, « Le blogue, un outil qui a du potentiel - Utilisations pédagogiques du blogue », RECIT, 17 nov. 2011, en ligne : <http://www.recit.qc.ca/article/utilisation-p%C3%A9dagogique-du-blogue> (site consulté le 3 mars 2012).

88 « Usage pédagogique », Vous avez dit blogue?, en ligne : <http://www.crdp-strasbourg.fr/b_usages/> (site consulté le 26 mai 2010).

Des blogues utilisés comme portfolio peuvent aussi être créés et gérés en collaboration, par plusieurs élèves en équipe dans un projet[89].

L'enseignant peut également se créer un blogue où il aura la possibilité de publier des liens Internet intéressants, de l'information, des réflexions et des travaux par rapport à un cours ou une recherche[90]. Et comme le support technologique est un blogue, les élèves ont la possibilité de publier des commentaires et faire des suggestions.

Le blogue de la classe est lui aussi créé par l'enseignant. Il « est le fruit d'une collaboration entre les élèves et les enseignants »[91]. Il sera très certainement géré par l'enseignant, mais il permet autant à ce dernier qu'aux élèves de publier du contenu. On peut y traiter d'activités scolaires et parascolaires – productions avec photos et commentaires[92]. De plus, puisque les blogues permettent de créer des catégories de sujets, l'enseignant pourrait créer un nouveau sujet pour un projet particulier auquel tous les élèves seraient amenés à participer en publiant du contenu, tel un « [j]ournal de la vie […] de la classe », ou un journal lors d'un voyage de classe[93]. De même, l'enseignant pourrait l'utiliser afin d'afficher des « ateliers, de devoirs et d'exercices en ligne »[94]. Certains enseignants se servent même des blogues pour corriger les travaux de leurs étudiants en ligne. Finalement, le blogue est un excellent médium pour permettre aux élèves d'entrer en contact avec des élèves du monde entier[95].

L'établissement d'enseignement pourrait utiliser un blogue en tant qu'outil de liaison avec les parents pour diffuser de l'information sur l'école: les projets, les activités, l'agenda scolaire, les congés[96].

---

89 « Usage pédagogique », Vous avez dit blogue ?, en ligne : <http://www.crdp-strasbourg.fr/b_usages/> (site consulté le 26 mai 2010).

90 Sonia SEHILI, « Le blogue, un outil qui a du potentiel - Utilisations pédagogiques du blogue », RECIT, 17 nov. 2011, en ligne : <http://www.recit.qc.ca/article/utilisation-p%C3%A9dagogique-du-blogue> (site consulté le 3 mars 2012).

91 Sonia SEHILI, « Le blogue, un outil qui a du potentiel - Utilisations pédagogiques du blogue », RECIT, 17 nov. 2011, en ligne : <http://www.recit.qc.ca/article/utilisation-p%C3%A9dagogique-du-blogue> (site consulté le 3 mars 2012).

92 Sonia SEHILI, « Le blogue, un outil qui a du potentiel - Utilisations pédagogiques du blogue », RECIT, 17 nov. 2011, en ligne : <http://www.recit.qc.ca/article/utilisation-p%C3%A9dagogique-du-blogue> (site consulté le 3 mars 2012).

93 « Vous avez dit blogue ? – Usage pédagogique », en ligne : <http://www.crdp-strasbourg.fr/b_usages/> (site consulté le 26 mai 2010).

94 « Usage pédagogique », Vous avez dit blogue ?, en ligne : <http://www.crdp-strasbourg.fr/b_usages/> (site consulté le 26 mai 2010).

95 Par exemple, voir : <collegien.blogspot.com>.

96 « Usage pédagogique », Vous avez dit blogue ? en ligne : <http://www.crdp-strasbourg.fr/b_usages/> (site consulté le 26 mai 2010).

Les blogues peuvent aussi servir comme source d'information pour les élèves dans le cadre de leurs travaux scolaires. On aura donc parfois des élèves qui publieront sur un blogue (le leur, celui de leur professeur ou celui de la classe), des informations tirées d'un autre blogue.

2. Quels sont les risques associés aux blogues ?

Cette section aborde les enjeux juridiques liés au fait de diffuser des contenus, généralement écrits, de façon **personnelle, publique** et **informelle** sur des sites permettant des échanges entre les internautes, notamment par la possibilité de faire des **commentaires**. Notons que les forums de discussions et babillards entrent aussi dans cette catégorie puisqu'ils partagent des enjeux similaires.

a. La divulgation de renseignements personnels

Un des plus grands risques des blogues est la facilité avec laquelle il est possible d'y dévoiler des renseignements personnels nous concernant ou concernant les autres. En effet, plusieurs personnes utilisent les blogues pour raconter des anecdotes ou encore parler de leur vie personnelle comme ils le feraient dans un journal intime. Il devient risqué à ce moment que des informations, comme une adresse de courrier électronique ou encore un numéro de téléphone, soient dévoilées, que ce soit volontairement ou non. La divulgation de coordonnées personnelles doit être faite avec précaution.

Cette possibilité de dévoiler des renseignements personnels devient problématique lorsque ce sont des personnes d'âge mineur qui créent un blogue ou qui y participent. La popularité croissante des blogues n'échappe pas aux enfants ou aux adolescents. Ils ne sont pas nécessairement conscients des risques qu'ils peuvent courir en dévoilant des informations personnelles sur Internet.

Les blogues deviennent pour certains un espace où raconter des histoires intimes, ce qui peut générer des atteintes à la vie privée. Souvent sous le couvert de l'anonymat, les internautes se croient permis de raconter des histoires intimes, parfois en nommant les personnes impliquées ou en donnant des détails qui peuvent les rendre identifiables. Par exemple, une dame qui tient un blogue où elle discute de sa vie sociale ainsi que des relations sexuelles qu'elle entretient avec des hommes pourrait porter atteinte à la vie privée des personnes avec qui elle a des relations. Si elle n'a pas leurs consentements pour publier ces informations intimes, elle s'expose à des poursuites judiciaires.

Questions à vérifier
- *Le blogueur est-il amené à dévoiler des renseignements personnels sur lui-même ou sur une autre personne ?*
- *Le blogueur est-il au courant des risques inhérents à l'utilisation de cet outil ?*
- *Est-ce qu'il y a un contrôle sur l'âge des participants ?*

b. Les atteintes à la réputation, la propagande haineuse et les menaces

Un blogue peut être un moyen facilitant la diffusion d'informations susceptibles de constituer des atteintes à la réputation, de la propagande haineuse, ou des menaces. En effet, aucune connaissance technique n'est vraiment requise pour y publier des textes et il s'agit là d'un média accessible à un grand nombre de personnes. De plus, les sites d'hébergement de blogues offrent habituellement ce service gratuitement. Comme les personnes se sentent invulnérables et anonymes sur Internet, cela peut contribuer à choisir ce média pour effectuer des actes illicites. Par contre, le blogueur est le premier responsable du matériel qu'il publie.

Dans ces conditions, une personne mal intentionnée peut facilement promouvoir, au moyen de son blogue, des idées qui peuvent constituer une atteinte à la réputation d'une personne, comme des insultes ou des propos humiliants. Par exemple, dire qu'un politicien souffre de détérioration mentale et qu'il est paranoïaque pourrait être considéré comme une atteinte à la réputation.

Il est facile aussi de diffuser des propos racistes et homophobes, constituant de la propagande haineuse, qui est d'ailleurs sanctionnée aux articles 318 et 319 du *Code criminel*. Une personne peut aussi menacer quelqu'un sur son blogue en diffusant, par exemple, des menaces de causer la mort. La propagation de menace est également un crime prévu à l'article 264.1 du *Code criminel*.

Dans certains cas, des personnes utilisent un blogue sous le nom de quelqu'un d'autre dans le but de nuire à la personne dont ils ont pris l'identité. Cela peut être fait notamment par l'ajout de photos compromettantes en ligne ou alors en attribuant des propos gênants. Dans le monde de l'éducation, il arrive fréquemment que des élèves parlent en mal de leurs professeurs ou de leurs membres de direction sur leurs blogues. Dans ces cas, les blogues ont des implications similaires aux sites de réseautage social, avec l'enjeu supplémentaire de la diffusion au grand public.

Questions à vérifier
- *Est-ce que les faits présentés sur le blogue sont vérifiés et vérifiables ?*
- *Est-ce qu'il y a présence de modération sur le site ?*
- *Quel est le sujet traité sur le blogue ? Est-ce un sujet en particulier ?*
- *Sommes-nous appelés à révéler des renseignements personnels sur notre blogue ?*

c. La diffusion des images des personnes

Lorsque le blogue présente des photographies, il y a un risque d'atteinte au droit à l'image de la personne. Les blogues personnels, par exemple, contiennent parfois des photographies des amis du blogueur ou d'événements auxquels il a participé avec d'autres personnes. L'utilisation de ces images, lorsque les personnes photographiées sont identifiables, risque de brimer leur droit à l'image. Une photo d'une personne ne peut donc pas être utilisée si l'individu concerné n'a pas donné son consentement.

L'insertion, dans son blogue, d'un lien qui mène vers la photographie de quelqu'un pourrait même être une source de litige possible.

d. Les atteintes au droit d'auteur

De plus, le blogueur peut parfois emprunter des images ou des oeuvres provenant d'autres sites Internet ou ailleurs. Des questions de droit d'auteur et de droit des marques de commerce peuvent alors se poser. En effet, pour publier une œuvre à l'égard de laquelle on ne détient pas les droits, il faut obtenir la permission de celui qui détient ces droits selon la *Loi sur le droit d'auteur*. Cette permission peut parfois s'avérer difficile à obtenir, en particulier pour les images puisqu'elles peuvent être reproduites d'un site à l'autre. On peut ainsi perdre la trace de la provenance initiale de l'œuvre.

Un blogueur américain a été condamné à un an de probation pour avoir mis en ligne neuf chansons tirées de l'album *Chinese Democracy* de Guns N' Roses. La Cour fédérale a aussi obligé le blogueur à enregistrer un message antipiratage pour la *Recording Industry Association of America*[97]. En France, Google a été condamné à verser des dommages à Benetton pour les comportements illicites d'une blogueuse qui reproduisait sur son blogue, hébergé par Google, la marque Benetton et des photos issues du catalogue[98].

Lorsqu'on établit des liens hypertextes, il faut également s'assurer de respecter le droit d'auteur. Des techniques consistant à reproduire le site à l'intérieur du blogue (*framing*) ou encore à copier la banque de liens hypertextes d'un autre site peuvent s'avérer risquées.

Questions à vérifier

- *Est-ce que les articles du blogue contiennent des œuvres ou parties d'œuvres qui sont protégées par la* Loi sur le droit d'auteur *?*
- *Est-ce que le blogueur détient les autorisations nécessaires pour publier tout ce qui se trouve sur son blogue ?*

e. La présence de contenu ne convenant pas aux enfants

Il est possible qu'un enfant, en naviguant sur des blogues, accède volontairement ou non à du contenu inapproprié ou ne convenant pas à son âge, comme de la

97 Anthony MCCARTNEY, « Un blogueur écope d'un an de probation pour avoir violé le droit d'auteur », Associated Press, Technaute.ca, 14 juillet 2009, en ligne : <http://technaute.cyberpresse.ca/nouvelles/internet/200907/14/01-884129-un-blogueur-ecope-dun-an-de-probation-pour-avoir-viole-le-droit-dauteur.php> (site consulté le 25 mai 2010).

98 *Google Inc. / Benetton*, Bencom, Cour d'appel de Paris 14e chambre, section A, 12 décembre 2007. Après que Benetton ait signalé les contenus manifestement illicites, l'hébergeur Google n'a pas agi promptement pour rendre inaccessible le blogue litigieux et a donc vu sa responsabilité engendrée pour les dommages causés.

pornographie ou encore des messages de violence. Puisque certains blogues couvrent des dizaines de sujets différents et non un seul en particulier, il devient difficile d'éviter complètement l'exposition à un contenu offensant. Il est possible, par exemple, de naviguer sur un blogue traitant de voyage et se retrouver sur un récit à caractère sexuel. Il y a par contre des sites d'hébergement de blogues qui sont consacrés uniquement à la publication de contenu à caractère sexuel, il devient donc plus facile d'éviter ces sites si tel est notre intention.

La pornographie ne convient généralement pas à un certain auditoire comme les enfants, mais elle n'est pas nécessairement illicite. Par contre, nous pouvons retrouver sur un blogue du contenu illégal, qui peut prendre la forme de matériel obscène, de bestialité ou encore de pornographie juvénile.

Questions à vérifier

- *Quel est le sujet du blogue en question ? Est-ce que le sujet convient au public qui est visé ?*

f. La consultation décontextualisée

Dans certains cas, tenir un blogue permet de montrer son savoir-faire à des employeurs potentiels ou tient lieu d'autopromotion. Or, parfois des blogueurs relatent des histoires sur leur vie professionnelle ce qui peut conduire à des réprimandes et même à un congédiement.

Au Québec (comme dans plusieurs autres endroits), l'employeur mécontent du blogue tenu par un employé peut congédier celui-ci, et ce sans préavis si ses propos constituent une faute grave ou si l'employé a manqué à son devoir de loyauté (par exemple, en divulguant un secret professionnel ou en tenant des propos insultants sur la compagnie).

Contrairement aux sites de réseautage social, le caractère généralement public des blogues empêche toute attente raisonnable de respect de la vie privée par l'employé face à son employeur ou son potentiel employeur, et ce même s'il agit anonymement.

Le professeur Erik Ringmar, de la *London School of Economics* (LES) a été réprimandé pour avoir publié sur son blogue les propos de la conférence qu'il avait donnée pour faire la promotion de son établissement auprès d'étudiants potentiels. À un moment de son discours, il disait qu'en raison de l'importance accordée à la recherche, les professeurs étaient peu disponibles et qu'essentiellement, c'était les étudiants au doctorat qui dispensaient la formation. Le directeur de son département ainsi que le

directeur général de LES l'ont sommé de retirer le billet « diffamatoire » de son blogue, ce qu'il a fait, tout en déplorant l'accroc à la libre expression[99].

g. La responsabilité pour les informations diffusées

Responsabilité du blogueur pour les textes qu'il publie

Un blogueur est pleinement responsable de l'information qu'il publie lui-même sur son blogue. Il a le contrôle sur ce qui est écrit dans les textes qu'il publie et il peut décider qui aura accès à la diffusion. Dans cette situation, il peut être qualifié d'éditeur, ce qui fait en sorte que les exonérations de responsabilités prévues dans la *Loi concernant le cadre juridique des technologies de l'information* ne s'appliqueront pas à lui.

Responsabilité du blogueur face aux commentaires de tiers

À l'égard des commentaires publiés par des tiers sur le blogue, des distinctions doivent être faites. Un blogueur qui exerce une modération attentive de tous les commentaires pourrait être tenu responsable si des propos illicites se retrouvent publiés. Dans une pareille hypothèse, l'on peut en déduire qu'il a approuvé les commentaires. Si le blogueur n'exerce pas de modération, ce n'est que lorsqu'il aura été est informé de la présence sur son blogue d'un document illicite qu'il aura l'obligation d'agir et de le retirer si nécessaire[100].

Question à vérifier
- *Est-ce que le blogueur a accès à un système de modération des commentaires sur son blogue ? Est-ce que cette fonction est activée ?*

h. L'utilisation des blogues à des fins judiciaires ou disciplinaires

Les moyens de communication sont de plus en plus élaborés et faciles d'accès, que ce soit la tenue d'un blogue personnel ou la prise d'images (vidéos, photos). De plus, il est désormais beaucoup plus facile de les conserver en ligne.

Tout propos exprimé sur un blogue et accessible au public peut éventuellement servir en preuve dans le cadre de procédures judiciaires. Ainsi, des photos ou vidéos mis en ligne volontairement peuvent se révéler problématiques pour leur auteur s'ils présentent des infractions ou minent leur crédibilité.

---

[99] Donald MACLEOD, « Lecturer's blog sparks free speech row », *The Guardian*, 3 mai 2006, en ligne: <http://www.guardian.co.uk/education/2006/may/03/highereducation.economics> (site consulté le 3 mars 2012).

[100] *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, art. 22.

3. Comment évaluer ces risques ?

La portée des risques que représentent les blogues sera plus ou moins importante selon ces facteurs : la présence de modération, l'anonymat des participants, le sujet traité et la présence de sons, d'images ou encore de vidéos.

a. La présence de modération

Lorsqu'il y a présence de modération sur le site, les risques sont minimisés. La modération peut se faire *a priori*, c'est-à-dire avant que le message soit publié sur Internet, ou encore *a posteriori*, qui signifie que le message sera immédiatement publié, avec la possibilité de le retirer si le contenu est jugé illicite.

S'il n'y a pas de modération sur le blogue, c'est lorsqu'il a connaissance du caractère illicite d'un propos publié que le blogueur a l'obligation d'agir et de le retirer si cela s'avère nécessaire (art. 22, *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1)

Question
- *Est-ce que le blogue est modéré ? Si oui, de quelle façon ? Cela se fait-il avant ou après la publication d'un commentaire ?*

b. Le caractère anonyme ou non des participants

L'anonymat des personnes qui tiennent un blogue ou qui commentent les billets des autres est aussi un facteur qui accentue les risques. Généralement, les hébergeurs recueillent certains renseignements personnels, comme l'adresse IP du blogueur et de ceux qui publient des commentaires. Ils peuvent proposer également au blogueur, au sein du service de modération, d'interdire les commentaires anonymes. On peut, par exemple, restreindre la possibilité de commenter les billets aux seuls membres du site Internet.

Par contre, lorsqu'il n'y a aucune mesure de contrôle, la publication de billets ou de commentaires au contenu illicite est facilitée puisque l'auteur sait qu'il est difficile de le retracer. Pourtant, il existe des moyens légaux et techniques pour retracer les auteurs anonymes et plusieurs ont été menacés devant les tribunaux de voir leur identité dévoilée et ainsi être appelés à répondre des informations illicites qu'ils ont mises en ligne.

Questions à vérifier
- *Est-ce que les participants communiquent dans l'anonymat ?*
- *Est-ce que les participants utilisent des pseudonymes ?*
- *Est-ce qu'il y a des restrictions quant aux personnes pouvant publier un commentaire ?*

c. Le sujet traité

Le traitement de certains sujets est plus risqué que d'autres. Il n'y a pas toujours un sujet précis qui est traité dans un blogue. Bien souvent, c'est un mélange de plusieurs sujets, qui peuvent varier entre l'actualité et la vie personnelle du blogueur, au gré de ses intérêts. Une personne peut donc avoir accès à un billet ne convenant pas à son âge, par simple inadvertance. Par contre, lorsqu'un sujet en particulier est développé sur un blogue, par exemple un sujet « chaud », il convient de faire preuve de prudence et de s'assurer que le contenu du site est convenable pour le public visé.

Questions à vérifier
- *Est-ce que le blogue traite de sujets qui sont définis clairement ? Est-ce qu'il y a plusieurs sujets ou est-ce un sujet en particulier ?*
- *Est-ce que le sujet traité convient à l'âge des participants ?*

d. La présence de sons, d'images ou de vidéos

Lorsqu'un blogue fait appel à des sons, images ou vidéos, peuvent s'ajouter des risques d'atteinte aux droits d'auteur ou aux droits des marques, si les éléments utilisés n'appartiennent pas au blogueur ou s'ils ne sont pas autorisés.

Les blogues peuvent aussi contenir la photographie du blogueur, ou de toute autre personne, comme les participants. Des problèmes de divulgation de renseignements personnels peuvent alors se poser ainsi que de droit à l'image.

Questions à vérifier
- *Est-ce qu'il y a présence de sons, d'images ou de vidéos sur le blogue ? Si oui, est-ce que le blogueur détient les autorisations nécessaires pour les utiliser ?*
- *Est-ce que le blogue présente l'image des participants ?*

4. Quelles sont les précautions à prendre ?

a. Établir une politique d'utilisation du site d'hébergement de blogues

Le site d'hébergement de blogues doit établir des règlements quant à l'utilisation de son service. Il pourrait, entre autres, interdire les blogues à caractère sexuel ainsi que ceux qui propagent un message de racisme ou de violence. Si les conditions d'utilisation ne sont pas respectées, le site peut se réserver le droit de fermer le blogue.

b. S'assurer, en créant un blogue, que l'hébergeur choisi offre un système de modération

La modération est importante pour éviter que des commentaires désobligeants se retrouvent sur un blogue. En choisissant un hébergeur de blogue, il est prudent de s'assurer qu'il fournit un service de modération complet, par exemple en limitant la

publication de commentaires aux seuls membres du site ou en offrant la modération *a priori*. Au minimum, il faut s'assurer que les tiers qui estiment qu'un document sur le blogue est illicite puissent le notifier au responsable du blogue afin que celui-ci retire le contenu lorsque son caractère illicite est confirmé.

c. Énoncer les règles de conduite des participants ou Nétiquette

Comme il est difficile de délimiter ce qui constitue un comportement interdit de ce qui relève de l'exercice de sa liberté d'expression, des règles de conduite doivent être énoncées pour informer les participants des propos et gestes qui sont considérés comme inacceptables sur le site. Par exemple, un blogueur peut, dans ses règles de conduite ou sa Nétiquette, avertir les participants qu'il est interdit de publier des commentaires qui portent atteinte à la réputation de personnes identifiables.

Une politique d'utilisation d'un blogue[101] doit indiquer aux tiers qu'ils sont responsables des propos qu'ils diffusent, et se réserver le droit de retirer des commentaires qui seraient contraires à la loi. La modération *a priori* des commentaires implique un choix éditorial qui pourrait rendre le blogueur responsable des contenus publiés par les tiers.

Il faut également indiquer un moyen de rejoindre l'auteur du blogue, et encourager les internautes à dénoncer les contenus contraires à la loi, que ce soit de la diffamation ou de l'incitation à la haine.

d. Informer les participants des risques liés à l'usage des blogues

Il est important de sensibiliser les participants aux risques auxquels ils s'exposent en utilisant les blogues, que ce soit pour la protection de leurs renseignements personnels ou pour la protection du droit d'auteur. Cette éducation doit se faire en particulier lorsque le public visé est composé d'enfants.

e. Pratiques pour minimiser les risques d'atteintes aux droits

Il faut éviter de mettre en ligne du contenu (texte, photo, dessin, vidéo, etc.) pour lequel on n'a pas les droits ou la permission du détenteur de droits.

Si l'objet (image ou vidéo) résulte d'un travail en équipe, il faut s'assurer que les co-blogueurs ne contreviennent pas au droit d'auteur, car tous pourraient être tenus solidairement responsables. De plus, lors d'un partage de blogue (par exemple si trois personnes rédigent un blogue), la personne qui écrit un texte conserve le droit d'auteur sur ce texte, mais le site entier est une œuvre collective (ensemble des billets et des commentaires, structure et apparence du blogue, etc.). Cela signifie que si un co-blogueur décide de quitter le blogue, il peut exiger le retrait de tous ses billets et, dans certaines circonstances, empêcher la continuation du blogue tel qu'il se présentait

---

101 Voir par exemple la politique du réseau Canoë, en ligne au <http://blogue.canoe.com/?disp=reglements>.

jusqu'alors[102]. Il peut être intéressant de conclure une convention entre les blogueurs ou, si le blogue est à but lucratif, de former une compagnie.

Souvent, l'objectif d'un blogue est d'échanger des informations et contenus avec les autres. Sur son blogue, le blogueur devrait indiquer clairement aux internautes son point de vue sur la question, par exemple si l'internaute doit demander une permission avant de reprendre ses propos.

Il faut distinguer ce qui relève de sa vie privée de ce qui relève de la sphère publique. Curieusement, beaucoup de blogues constituent des journaux intimes publics. Il faut alors utiliser son jugement et veiller à protéger l'intimité des personnes impliquées dans les histoires personnelles racontées[103].

D. Le micro-blogue (Twitter)

1. Qu'est-ce qu'un micro-blogue (Twitter) ?

À l'instar d'un blogue, Twitter permet de publier des messages sur une page qui nous est attitrée. Contrairement au blogue traditionnel, le nombre de caractère est limité à 140 par message. Pour cette raison, on catégorise Twitter comme site de *micro-blogging*.

Twitter permet ensuite de s'abonner à d'autres utilisateurs, ce qui permet de les *suivre*. Ainsi, lorsque l'utilisateur ouvre sa page d'accueil, il y retrouve un fil de nouvelles avec tous les messages récents de ses abonnements.

Il convient de signaler que tous les *tweets*, c'est-à-dire messages de moins de 140 caractères, sont *a priori* publics. Nul besoin d'être membre pour lire des messages sur Twitter. L'adhésion au service est gratuite et permet simplement de suivre et d'être suivi par d'autres utilisateurs.

Certaines fonctions rendent l'utilisation de Twitter plus efficace. Il est possible de *Retweeter* un *tweet* que nous recevons sur notre page d'accueil afin d'en faire part à ceux qui nous suivent. On peut répondre aux messages qui apparaissent sur notre page d'accueil. Un utilisateur peut aussi envoyer un message sur la page de profil d'un autre en commençant son message par le symbole @ suivi du nom de l'utilisateur.

Une des fonctions du micro-blogue Twitter est le *hashtag*. Un *hashtag* est un mot-clé précédé du symbole dièse (#). Il sert à répertorier tous les commentaires traitant d'un sujet. Ainsi, un utilisateur pourra utiliser le moteur de recherche afin de trouver un

---

102 Eric GOLDMAN, « Co-Blogging Law », 84 Washington University Law Review 1169, en ligne depuis le 20 avril 2006 : <http://ssrn.com/abstract=898048> (site consulté le 25 mai 2010).

103 Voir par analogie, *Aubry c. Éditions Vice-Versa inc.*, [1998] 1 R.C.S. 591.

hashtag portant sur un sujet qui l'intéresse. En cliquant sur ce *hashtag*, qui prend la forme d'un lien hypertexte, il se retrouvera sur une page qui répertorie, du plus récent au plus ancien, tous les commentaires publiés en lien avec ce sujet.

Le contenu des publications sur Twitter diffère de celui des blogues ou autres outils du Web 2.0. Comme les messages se limitent à 140 caractères, il est d'usage de mettre des hyperliens, afin de rediriger ses lecteurs sur d'autres sites.

Enfin, Twitter permet aussi la création de listes d'abonnements. Les listes d'abonnements peuvent être publiques ou privées. Lorsqu'elles sont publiques, elles peuvent être partagées. Par exemple, un utilisateur peut créer une liste *Université* et ajouter tous les professeurs qu'il connaît qui ont un compte Twitter.

a. Qui fait quoi ?

i) Les usagers

Les particuliers utilisent généralement Twitter pour échanger, partager ou commenter sur toutes sortes de sujets, y compris la vie quotidienne. Les usagers peuvent aussi personnaliser leur page de profil au moyen de photos, de fonds d'écran ou du choix de la couleur de la police.

Les usagers sont généralement des personnes. Il arrive de plus en plus que les compagnies s'abonnent à Twitter pour créer des campagnes promotionnelles de type viral ou pour obtenir la rétroaction du public sur certains produits ou services. Les entreprises peuvent aussi payer pour des *Tweets* publicitaires qui seront diffusés sur les pages d'accueil de certains abonnés.

Certaines personnes célèbres bénéficient d'un symbole indiquant que leur compte a été validé. Le compte validé indique que c'est le compte Twitter officiel de la personne. Bien que ce procédé ne soit encore réservé qu'à des célébrités, elles peuvent aider à prévenir l'hameçonnage.

Tous les usagers sont soumis à la *Politique d'utilisation de* Twitter, qui comprend un code de conduite ainsi qu'une politique de confidentialité. Contrairement à la plupart des sites où une adhésion est requise, Twitter ne prévoit pas de minimum d'âge[104].

ii) Les visiteurs

Les visiteurs sont tous ceux qui visitent ou consultent Twitter sans y participer en tant que membre. Les visiteurs ont accès aux *Tweets* de tous les membres, à l'exception des profils privés. Ils ont aussi la possibilité d'effectuer des recherches. De plus, chaque

104 Voir: Formulaire d'adhésion à Twitter. Conditions d'utilisation de Twitter, en ligne : <http://twitter.com/tos>.

compte Twitter est muni d'un fil de syndication de données (RSS). Il est donc possible pour un visiteur de suivre les *Tweets* d'un membre sans s'abonner à Twitter.

Les visiteurs peuvent aussi trouver le profil d'un membre de Twitter par un moteur de recherche. À l'instar de la plupart des blogues, chaque compte Twitter est accessible via une adresse URL.

Contrairement au blogue ordinaire, les visiteurs sur Twitter occupent une moins grande place que les abonnés.

iii) Les abonnés

Les abonnés regroupent tous les usagers membres de Twitter qui suivent un usager précis. Lorsque ce dernier publie un *Tweet*, tous ses abonnés voient le message sur leur page d'accueil.

Les abonnés peuvent aussi *Retweeter*. Cette fonction est très importante dans ce réseau. Twitter n'affiche pas le nombre de visites qu'une page a reçu, mais indique le nombre de fois qu'un message a été relayé par *retweet*.

iv) Les développeurs

Les développeurs sont ceux qui créent la plateforme de Twitter. Ils déterminent aussi le contenu de la Politique d'utilisation. Ils se réservent le droit d'intervenir lorsqu'une infraction aux conditions d'utilisation est signalée[105].

b. Utilisation du micro-blogue (Twitter) en éducation

Comme c'est le cas pour les blogues, les établissements d'enseignement, les enseignants, de même que les élèves peuvent trouver une utilité à se créer un compte Twitter.

Les établissements peuvent l'utiliser d'une façon semblable aux blogues, c'est-à-dire surtout pour tenir le public, les élèves et leurs parents informés de la vie de l'école[106]. Toutefois, Twitter permet une plus grande interaction, puisque n'importe quel usager peut envoyer un message à l'établissement.

Pour les enseignants, Twitter peut avoir des usages multiples. D'abord, un enseignant peut s'ouvrir un compte et y diffuser des informations à l'intention de ses élèves (liens

---

105 « Twitter : Conditions d'utilisation », *Twitter*, <http://en.twitter.com/tos>, Restriction sur le contenu et l'utilisation des services.

106 Sur ce sujet, voir Ministère de l'Éducation nationale de France, « Utiliser le micro-blogging en classe, un exemple en lycée professionnel », en ligne : <http://eduscol.education.fr/cid50815/micro-blogging-en-classe.html> : « Il permet de communiquer rapidement avec l'ensemble de la communauté éducative et ses partenaires, les familles par exemple. Il permet une ouverture de l'école sur le monde extérieur (entreprises, médias, autres établissements) ».

vers des sources documentaires, précisions sur les travaux à effectuer, activités à venir en classe, etc.). Les élèves, sans avoir besoin de s'inscrire sur Twitter, pourront aller chercher les informations en question. Cependant, pour qu'une telle utilisation soit possible, il faut que les messages de l'enseignant soient publics, donc accessibles à tous.

Si les élèves se créent également un compte Twitter, les enseignants ont plus de possibilités. De cette façon, les élèves peuvent interagir avec leur enseignant et entre eux sur des sujets reliés à l'école. Voici quelques possibilités qu'offre Twitter aux élèves :

- Publier des messages relatifs à un projet qu'ils doivent effectuer, accompagnés de liens qui renvoient à des sources documentaires.
- Suivre des organismes ou des personnes qui s'intéressent à leur sujet de recherche, de façon à se faire référer des informations différentes de celles qu'ils trouvent dans leurs recherches habituelles.
- Constituer et partager des listes d'abonnements d'usagers qui commentent pertinemment le sujet d'une recherche.
- Collaborer entre élèves sur un travail d'équipe.
- Se pratiquer à la prise de notes. Par exemple, durant la présentation d'un documentaire en classe, les élèves ont accès à Twitter et doivent répondre aux questions posées par leur enseignant.
- Communiquer avec leur enseignant à l'extérieur des heures de classe pour trouver réponse à des questions.
- Pour les enseignants, obtenir l'opinion des élèves sur certaines activités pédagogiques.

Une possibilité offerte par Twitter pour l'éducation est de faciliter les échanges avec d'autres classes (notamment, avec d'autres pays)[107].

Enfin, Twitter est de plus en plus pris au sérieux comme outil de consultation de l'actualité. Twitter perce souvent les nouvelles, et ce, avant les grands médias. À cet effet, le BBC College of Journalism rapporte que Twitter a joué un rôle crucial dans la couverture du séisme à Haïti en 2009. Par la suite, Twitter a été utilisé pour coordonner certaines opérations d'aide aux sinistrés. Il est envisageable que Twitter puisse être utilisé par les institutions scolaires dans leurs mesures d'urgence[108]. Donc, autant les enseignants que les institutions scolaires doivent comprendre l'importance et le

---

107 Kathleen Kennedy MANZO, « Twitter Lessons in 140 Characters or Less », *Education Week*, en ligne : <http://www.edweek.org/ew/articles/2009/10/21/08twitter_ep.h29.html?tkn=MRZF3k/zhIEfPW/2Nv9YbL2qQKm/Khfv8YFB>.

108 Matthew ELTRINGHAM, « Has Twitter grown up ? », *BBC College of Journalism Blog*, 28 mai 2010, en ligne : <http://www.bbc.co.uk/journalism/blog/2010/05/has-twitter-grown-up.shtml>, (site consulté le 31 mai 2010).

potentiel de cet outil. Il demeure primordial de comprendre les risques reliés à son utilisation.

2. Quels sont les risques associés au micro-blogue (Twitter) ?

a. La diffusion de renseignements personnels et les atteintes à la vie privée

Twitter invite l'usager à « converser ». La plupart des usagers partagent sur des sujets d'actualité, mais surtout conversent sur eux-mêmes, leur vie familiale, des gens qu'ils ont rencontrés, les endroits qu'ils fréquentent, etc.

Les risques sont similaires à ceux du blogue standard de révéler des informations personnelles sur soi-même ou sur autrui. Comme Twitter permet d'afficher tous les *tweets* d'un usager, il est envisageable d'identifier une personne en cumulant différents indices.

D'autant plus, Twitter ne prévoit pas de minimum d'âge pour adhérer au service. Comme il gagne en popularité chez les enfants et les adolescents, les risques sont grands que des informations personnelles soient divulguées. Comme la persistance des *tweets* sur Twitter est encore inconnue, les informations divulguées peuvent demeurer accessibles longtemps après leur publication.

Questions à vérifier

- *Quels renseignements personnels sont divulgués ? Nom complet ? Lieux de fréquentation ? Adresse ? Adresse courriel ?*
- *L'usager fournit-il des renseignements sur d'autres personnes ?*
- *Est-ce que la personne a consenti à ce qu'on donne des informations sur elle ?*
- *Est-ce que la personne est aussi abonnée à Twitter ?*
- *Est-ce que l'usager laisse suffisamment d'indices pour deviner qui est la personne visée (Surnom, lieu de travail, habillement, description physique) ?*

b. Les atteintes à la réputation, les propos haineux ou autrement inappropriés

Comme pour le blogue, les risques de diffusion de propos haineux, menaçants, propagandistes ou diffamatoires sont présents sur Twitter. Ces risques sont néanmoins accentués par le caractère décontextualisé qu'impose le maximum de 140 caractères. Une mauvaise blague peut rapidement être interprétée comme une menace.

Le risque est accentué par la fonction *Retweet*. Il est possible en tout temps d'effacer un *Tweet* que l'on a publié. Toutefois, lorsque le message a été republié, via *retweet*, par un autre usager, il n'est plus possible de le supprimer. Il est donc facile de perdre le contrôle sur un message.

De plus, l'usager ne se doute pas nécessairement qu'en 140 caractères, un message peut être lourd d'impacts. Par exemple, une dame aux États-Unis a été poursuivie pour 50 000 $ pour avoir *tweeté* que son appartement était maintenu dans des conditions

insalubres par la compagnie de gestion de l'immeuble[109]. La poursuite a cependant été rejetée, car le tribunal n'a pas jugé le propos diffamatoire. Mais le droit québécois est beaucoup plus protecteur de la réputation que le droit américain et les risques de poursuites pour des critiques adressées à une entreprise sont plus élevés.

Twitter présente aussi un risque particulier en ce qui concerne les propos haineux. Les usagers qui veulent avoir beaucoup d'abonnés, et qui ne sont pas des célébrités hors Twitter, vont souvent capitaliser sur un sujet particulier qu'ils traiteront à fond. Un usager peut trouver là une tribune pour des blagues à caractère raciste, sexiste ou méprisant à l'endroit de la religion, des handicapés, etc.

Questions à vérifier

- *L'usager identifie-t-il un groupe déterminé dans ses micromessages ?*
- *L'usager nomme-t-il les personnes visées par ses commentaires ?*
- *L'usager critique-t-il une pratique ou s'adonne-t-il plutôt à des attaques personnelles ?*
- *L'usager encourage-t-il à la haine ou le mépris d'un individu ou d'un groupe identifiable ?*

c. La redirection vers des sites à contenu inapproprié

Ce risque est causé une fois de plus du maximum de 140 caractères. Comme les liens vers les adresses URL des sites Web sont parfois longs, il est possible de les raccourcir. Le site le plus utilisé pour raccourcir les URL est sans doute <http://bit.ly>. Grâce à ce service, une adresse URL vers un article de journal, qui se lirait comme suit <http://news.bbc.co.uk/2/hi/business/10145993.stm> deviendrait <http://bit.ly/cnIj9E>.

Bien que cela semble très avantageux à première vue, on se rend vite compte que l'on perd le nom de domaine du site auquel on réfère. Outre la confiance en l'usager qui publie le lien, le nom de domaine est la seule référence que l'on a pour juger a priori de la qualité du lien. Il est risqué, dès que le lien est publié par un inconnu, d'être redirigé vers des tentatives d'hameçonnage, du contenu offensant, sexuellement explicite, violent ou autrement inapproprié. Heureusement, il existe de plus en plus de méthodes pour visualiser le lien en entier avant de cliquer.

Il est à noter aussi que la limite de 140 caractères sur Twitter n'est imposée que dans les *tweets*. Dans la page de profil d'un individu, le nombre de caractères est de 160. On y retrouve en plus un endroit spécifique pour inscrire une adresse URL au long. Il n'y a donc pas de raison de raccourcir une adresse URL dans une page de profil. Une adresse URL raccourcie inutilement présente un haut risque de contenu douteux.

---

109 AGENCE FRANCE-PRESSE, *Cyberpresse*, « Une poursuite de 50 000 $ pour un “ tweet ” diffamatoire », 31 juillet 2009, en ligne: <http://technaute.cyberpresse.ca/nouvelles/internet/200907/29/01-888214-une-poursuite-de-50-000-pour-un-tweet-diffamatoire.php> (site consulté le 3 juin 2010). Voir aussi : <http://en.wikipedia.org/wiki/Horizon_Group_v._Bonnen>.

Questions à vérifier

- *Est-ce qu'il est possible de vérifier l'adresse URL en entier avant de cliquer ?*
- *Est-ce que le message a un nombre de caractères limité ? Est-ce que le lien a une raison d'être raccourci ?*
- *Qui publie le lien ? Est-ce une personne de confiance ? A-t-il beaucoup d'abonnés ? Est-ce que des personnes de confiance sont abonnées à cet usager ?*
- *Le texte qui accompagne le lien en décrit-il le contenu ? Ou s'agit-il simplement d'une invitation à le suivre ?*

d. La consultation décontextualisée

Comme pour le blogue traditionnel, Twitter présente des risques que les commentaires écrits soient lus hors de leur contexte. Ce risque est accentué sur Twitter par deux particularités : le maximum de caractères et la fonction de recherche.

D'abord, comme le *tweet* ne peut comporter qu'un maximum de 140 caractères, l'usager doit aller à l'essentiel. Pour ce faire, il peut arriver qu'il omette le contexte ou les motifs qui le poussent à écrire son commentaire. Un exemple illustre bien les risques associés à la fonction de recherche. Si une entreprise désire savoir ce que les usagers pensent de ses produits et services, elle peut inscrire son nom dans la fonction recherche. Si un employé a écrit « Travailler pour cette compagnie est pénible », la compagnie lira ce commentaire sans explication ou contexte. Autre exemple: exaspéré d'avoir vu son vol repoussé, un Britannique a fait une blague noire sur Twitter au sujet de l'aéroport Robin Hood en insinuant qu'il devrait la faire exploser. Cette blague prise très au sérieux par les autorités lui a valu sept heures d'interrogatoire, la perte de son emploi et une amende de 1 000 Euros[110].

Ces deux caractéristiques, maximum de caractère et fonction de recherche, génèrent de grands risques de décontextualisation.

Questions à vérifier

- *L'information publiée est-elle confidentielle ?*
- *Les micromessages sont-ils médisants ?*
- *S'il s'agit d'humour, comprend-on bien qu'il s'agit d'une blague ? Et ce, même si le lecteur ne connaît pas personnellement l'auteur du message ?*

e. L'utilisation des messages à des fins judiciaires ou commerciales

La fonction *Retweet* augmente considérablement la persistance des informations sur Internet. Il y a donc de très hauts risques qu'une fois publié, le message persiste dans le cyberespace. Le message pourrait être utilisé en preuve dans le cadre d'une procédure judiciaire.

---

110 *BBC News South Yorkshire*, « Man in Twitter Bomb Threat against Airport Loses Appeal », 11 novembre 2010, en ligne: <http://www.bbc.co.uk/news/uk-england-south-yorkshire-11736785> (site consulté le 15 mars 2012).

Les conditions d'utilisation de Twitter prévoient que l'usager accorde une licence à Twitter[111]. L'usager perd la maîtrise exclusive de ce qu'il publie. Twitter se réserve le droit d'utiliser à sa guise les *tweets* à des fins commerciales. Jusqu'à maintenant, cette disposition ne semble pas avoir engendré de différends. Il existe tout de même un risque qu'un usager voit ses *tweets* servir à des fins commerciales ou publicitaires.

f. L'usurpation d'identité et l'hameçonnage

Les comptes Twitter peuvent être créés très facilement. N'est requise pour l'inscription qu'une adresse courriel valide. Un usager peut ainsi se faire passer pour une vraie personne et écrire des messages publics en son nom et ainsi causer des dommages.

L'usurpation d'identité est aussi utilisée pour hameçonner. Les usurpateurs créent un compte au nom d'une célébrité, accompagné d'une photo de celle-ci. Ils se constituent une grande liste d'abonnés. Plusieurs sont alors tentés de *suivre* la célébrité. Cette dernière envoie alors des messages publicitaires.

La compagnie de sécurité informatique Symantec rapporte le cas d'une utilisatrice de Twitter qui a vu apparaître dans ses abonnés le nom de David Beckham. Selon elle, le compte de Beckham avait l'air crédible, photo à l'appui. Il s'agissait en fait d'un cybermarchand chinois qui faisait la promotion de ses produits et qui fournissait une adresse pour aller sur son site[112]. Le Dalaï-Lama a aussi fait l'objet d'usurpation d'identité. Un faux compte Twitter a été créé en son nom[113].

g. Les atteintes au droit d'auteur

Le risque de violation de droit d'auteur est très mince sur Twitter. Pour ce faire, il faudrait que le tweet copié soit protégé par droit d'auteur. Or, il n'est pas certain que les 140 caractères suffisent pour produire une œuvre originale de l'esprit qui mérite d'être protégée[114].

Toutefois, un slogan publicitaire, les vers importants d'un poème ou d'une chanson pourraient faire l'objet d'une protection de droits d'auteur. Il convient d'obtenir l'autorisation avant de reproduire sur Twitter un tel contenu.

---

111 « Vos droits », *Twitter | Conditions d'utilisation*, <http://twitter.com/tos>, (site consulté le 31 mai 2010).

112 Candid WUEEST, « Becks Loves Me » *Symantec Connect*, 4 mai 2010, en ligne: <http://www.symantec.com/connect/fr/blogs/becks-loves-me> (site consulté le 15 mars 2012).

113 TECHNAUTE.CA, « Un faux Dalaï-Lama sur Twitter », *Cyberpresse*, 12 février 2009, en ligne : <http://technaute.cyberpresse.ca/nouvelles/internet/200902/10/01-825928-un-faux-dalai-lama-sur-twitter.php> (site consulté le 24 mai 2010).

114 *Loi sur le droit d'auteur*, L.R.C. 1985, c. C-42, art. 2.

3. Comment évaluer ces risques ?

a. L'usager a-t-il choisi des critères de confidentialité privés ?

Il est possible sur Twitter de paramétrer son compte à « privé ». Cela a pour effet de rendre les *tweets* seulement accessibles aux personnes que l'on a autorisées. En paramétrant ainsi le compte, Twitter ressemble plus à un réseau social où l'on peut choisir qui entre dans son cercle privilégié.

De paramétrer ainsi le compte d'un usager permet de réduire les risques de divulgation de renseignements personnels et d'utilisation des messages à des fins commerciales.

Toutefois, paramétrer ainsi le compte n'empêche aucunement l'usager d'avoir accès à tout ce qui se trouve sur Twitter. Ainsi, subsistent, avec la même intensité, les risques d'être redirigé vers du contenu inapproprié.

b. L'usager est-il «suivi» par un proche ou quelqu'un de confiance ?

L'usager qui est « suivi » par un proche, un enseignant ou une autre personne de confiance aura certainement plus tendance à faire attention à ce qu'il écrit. Il est donc possible pour un enseignant, si Twitter est utilisé en classe, par exemple, de s'abonner à ses élèves. Ces derniers savent alors que tout ce qu'ils publieront sur leur Twitter pourra être lu par leur enseignant ou leurs parents.

c. L'usager utilise-t-il un pseudonyme ?

Le pseudonyme sur Twitter est tout à fait permis. La plupart des usagers s'identifient par leur nom, car ils utilisent Twitter comme outil d'auto-promotion. Toutefois, un usager qui veut seulement utiliser Twitter pour converser avec ses amis est plus justifié d'utiliser un pseudonyme. Ce pseudonyme a pour effet de diminuer les risques de divulgation de renseignements personnels compromettants. En effet, il devient plus difficile de compiler des informations sur un usager lorsque son nom n'est pas indiqué.

Toutefois, il convient de rappeler que le pseudonyme ne réduit en rien les risques de poursuite pour diffamation ou de sanctions criminelles pour des propos inopportuns. Il peut même parfois accentuer ces risques en générant un sentiment d'invulnérabilité.

d. L'usager est-il conscient du caractère public de Twitter ?

L'usager doit être conscient que sur Twitter, ce n'est pas seulement un cercle étendu de personnes qui ont accès à ses dires, mais bien « tout le monde». Cette conscience n'est pas nécessairement reliée à l'âge puisque même des adultes oublient ce fait.

Principalement, il s'agit de se demander si l'usager sait que « tout le monde » inclut l'employeur, les médias, l'institution scolaire, les inconnus, etc.

4. Quelles sont les précautions à prendre ?

a. Informer les usagers des risques d'utilisation du micro-blogue

Twitter est accessible à tous depuis n'importe quel ordinateur relié à Internet. Il l'est aussi via un téléphone mobile relié à Internet. De plus, il est accessible aux usagers de tous âges. La page d'inscription, ainsi que les conditions d'utilisation, ne requièrent aucun âge minimal.

Twitter, contrairement aux réseaux sociaux, demande un effort de discernement constant. Comme l'information est entièrement publique, il faut être en mesure de se demander si l'information contenue dans le micromessage peut s'avérer compromettante.

Twitter demeure un outil très rapide et efficace pour l'échange d'information. Il convient de l'utiliser avec soin et prudence. Il faut sensibiliser les usagers aux risques auxquels ils s'exposent, en particulier lorsque ce sont des jeunes.

b. Sensibiliser les usagers aux bonnes pratiques et comportements

La protection de la vie privée d'autrui:

Lorsqu'un usager veut parler d'une autre personne, il est préférable d'identifier uniquement les individus membres de Twitter. Par exemple : « Je suis allé manger avec @YvonTremblay ».

Pour identifier les personnes qui n'utilisent pas Twitter, il est préférable de les présenter seulement par leur rôle. Par exemple, plutôt que d'écrire : « Je suis allé manger avec Jean Tremblay », il serait moins risqué d'écrire : « Je suis allé manger avec un bon ami/collègue/frère ».

L'institution scolaire ou l'enseignant qui utiliserait Twitter pour informer de ce qui se passe à l'école ne doit pas identifier un élève par son nom. Par exemple, « Bravo Jonathan Tremblay pour ton méritas! » serait interdit par la loi. Toutefois, il est envisageable de n'utiliser que le prénom : « Bravo Jonathan pour ton méritas ». Si toutefois le prénom est si peu courant qu'il identifie l'élève, il est préférable de ne pas le nommer du tout.

La protection de ses informations :

À tout moment, il convient de se rappeler que Twitter n'est pas un outil approprié pour échanger des secrets. Le contenu est entièrement public. Même si un compte est privé, il est possible pour ses abonnés de republier le contenu et de l'associer à son auteur.

La redirection vers des contenus inappropriés :

En présence de liens raccourcis sur Twitter, il convient d'abord de se demander qui publie le lien. La page de profil d'un membre ainsi qu'un aperçu de ses *tweets* sont souvent un indice de la qualité de ses publications.

Il convient aussi de vérifier si le membre a l'habitude d'accompagner ses liens de texte. Une simple invitation à suivre un lien (« Aller voir ça, c'est génial!!! http://bit.ly/exemple ») est un indice de haut risque.

Dès lors qu'un doute subsiste, il est approprié d'utiliser une extension Bit.ly ou autre. Une extension Bit.ly est un module complémentaire que l'on peut ajouter à son client de navigation. Ce module fait en sorte que les liens raccourcis vont s'afficher dans notre navigateur en version longue[115].

La consultation décontextualisée :

Ce risque peut se résoudre généralement par une seule question : « Y a-t-il des chances que ce que j'écris puisse déplaire ne serait-ce qu'à une seule personne, susceptible ou non d'utiliser Twitter ? ». Si la réponse est oui, il vaut mieux y repenser avant de publier le message. Il sera peut-être plus opportun de publier le message dans un autre réseau social ou via un autre moyen de communication.

Il est conseillé aussi d'éviter l'utilisation de l'ironie comme type d'humour. L'impossibilité de prendre connaissance du ton réel de la personne rend ce procédé humoristique très dangereux. De plus, il y a le risque que le message soit lu par des personnes qui supportent mal l'ironie.

Possibilité d'utilisation des micromessages à des fins judiciaires :

Tout ce qu'on dit sur Twitter peut être retenu contre nous. Ces micromessage peuvent facilement être mis en preuve devant un tribunal. Il importe donc de se rappeler de bien se comporter sur Twitter. Il peut s'avérer risqué d'utiliser Twitter pour évacuer ses frustrations ou se vanter de ses « mauvais coups ».

c. « Suivre » la personne sous notre garde

Il convient enfin de rappeler que la précaution la plus efficace pour minimiser les risques est probablement de « suivre » via Twitter la personne qui est sous notre garde.

[115] Denis HIRST, « 7 Conseils pour sécuriser votre utilisation de Twitter », *Le blog des internautes du XXIe siècle*, en ligne: <http://www.denishirst.fr/fr/2010/05/conseil-pour-s%C3%A9curiser-votre-utilisation-de-twitter.html#tp> (site consulté le 31 mai 2010).

E. Les sites de notation de personnes, de services ou de produits

1. Qu'est-ce qu'un site de notation ?

Un site d'évaluation de produits et de services offre généralement au public la possibilité d'évaluer et de commenter un service reçu ou encore un bien acheté. Des sites vont également proposer d'octroyer une note aux attributs physiques d'une personne ou encore à une panoplie de biens, comme des voitures ou des animaux. La soumission d'une évaluation est facile, il suffit généralement de cliquer sur un lien, parfois nommé « *Rate this* », « *Rate My…* » et ensuite remplir le formulaire d'évaluation.

Un des buts recherchés par ces sites est d'informer les personnes intéressées par un produit ou un service sur la qualité de ce dernier ou à tout le moins sur ce que les autres pensent de ce produit ou service. Les gens qui évaluent sont généralement des personnes qui ont acheté ou utilisé le bien ou le service en question. Les consommateurs qui ont accès à ces évaluations peuvent donc prendre une décision plus éclairée avant de faire un achat. Une personne qui veut se procurer une bicyclette, par exemple, ne choisira probablement pas d'acheter la marque qui s'est méritée une centaine de commentaires négatifs. Elle choisira plutôt la marque qui a reçu des évaluations positives. De la même façon, les gens ne seront pas portés à requérir les services d'un notaire auquel on aurait attribué plusieurs commentaires négatifs.

Les sites d'évaluation de personnes ont plutôt pour but de divertir le public en proposant d'évaluer la beauté des gens qui ont soumis leur photographie. Ces personnes sont évaluées au moyen d'une note qui est habituellement de 1 à 10. Certains proposent ensuite un classement des individus ainsi jugés. D'autres offrent un service de rencontre en mettant en relation un membre du site et un visiteur séduit par le membre en question.

Les modes d'évaluation des biens ou services soumis peuvent être extrêmement différents d'un site à l'autre. Certains proposent un système de notation sur une échelle de 1 à 10, d'autres attribuent cinq étoiles ou moins au bien en question. On peut aussi dans certains cas laisser un commentaire avec l'évaluation soumise. Généralement, les évaluations soumises sur ces sites ne peuvent pas être retirées par l'auteur lui-même. Seuls les administrateurs du site peuvent les supprimer, sur justification de la demande. De plus, certains sites permettent d'évaluer une seule fois un produit ou une personne, tandis que d'autres permettent de l'évaluer un nombre de fois indéfini.

L'adhésion à un tel site d'évaluation peut être volontaire ou non. Habituellement, les sites d'évaluation de services reçus ne sont pas basés sur une procédure d'inscription volontaire. Ce sont les personnes qui ont reçu le service qui inscrivent sur le site le nom du service reçu et l'appréciation qu'ils en donnent. Par exemple, sur le site *RateMyProfessors.com*, qui évalue l'enseignement de certains professeurs, ce sont des

élèves qui ajoutent les noms de professeurs à la base de données du site et non les professeurs eux-mêmes.

De la même façon, plusieurs sites de commerce électronique, comme eBay, incorporent au service de vente une évaluation des produits vendus, des vendeurs et des acheteurs. L'adhésion à cette procédure de notation n'est pas volontaire, elle est obligatoire si nous voulons faire affaire sur le site. Ces évaluations permettent ensuite de savoir si un vendeur est apprécié des autres usagers du site, ou si l'acheteur avec qui nous faisons affaire n'est pas en retard lorsqu'il paie des articles.

Par contre, l'adhésion à certains types de sites d'évaluation sera totalement volontaire. Ces sites consistent généralement à évaluer les attributs physiques d'une personne (ex. : <http://www.hotornot.com/>) ou encore des biens en sa possession comme un animal ou une voiture (ex. : <http://www.ratemyride.com/>). Il suffit de soumettre une photographie, qui sera ensuite publiée sur le site, pour que le public l'évalue.

a. Qui fait quoi ?

i) Les usagers

Les usagers jouent un rôle fondamental dans les sites de notation. Ce sont eux qui mettent en ligne les avis et les cotes qui constituent le fondement même de l'existence des sites d'évaluation.

ii) Les personnes, organismes ou entreprises évalués

Tous les sites de notation ont une chose en commun, soit celle d'évaluer un objet en particulier. Dans certains cas, ce sont des personnes, dans d'autres des services et pour quelques autres ce sont des biens. Dans tous les cas, ces « objets » seront notés par les usagers des sites.

Une personne peut décider de mettre en ligne une photo ou vidéo d'elle-même pour qu'elle soit notée par les autres; l'usager sera dans ce cas la personne évaluée. Elle peut également mettre en ligne la photo de quelqu'un d'autre – notamment par le biais de sites comme Dontdatehimgirl.com. Dans ce cas, la personne n'a pas décidé de se retrouver en ligne. C'est d'ailleurs le processus normal pour les sites de notation. Certains sont dédiés aux travailleurs ou aux professionnels, notamment les dentistes, médecins, avocats, comptables, etc.

Aussi, il existe des sites permettant aux employés d'évaluer leur entreprise, et ce, anonymement. D'autres sites évaluent les restaurants, la qualité de la nourriture, le service et l'expérience qu'on y a vécue.

iii) Les sites de notation

Les sites de notation offrent le cadre dans lequel on peut ajouter des évaluations et des informations sur un « objet » donné. La qualification de ces sites n'est pas claire. Sont-ils des éditeurs ou des hébergeurs ? La responsabilité qui en découlera sera bien différente et les enjeux sont majeurs vu la nature controversée des sites de notation. Par exemple, un site qui participe à l'édition de contenu en proposant des critères et catégories ou en proposant des réponses pré-rédigées pourrait être plus qu'un simple hébergeur et être qualifié d'éditeur. Par contraste, le site de notation qui laisse aux usagers le soin de noter à leur guise pourra aisément être traité au regard de la loi comme un intermédiaire de type « hébergeur ».

b. Utilisation des sites de notation en éducation

Les sites de notation sont un instrument privilégié pour les étudiants quand vient le temps de donner leurs opinions sur leurs professeurs. C'est plutôt à ce niveau que les sites d'évaluation peuvent poser des risques.

Certains sites de notation sont spécialement créés pour l'évaluation des professeurs. Pensons notamment au défunt *Note2be.com* et à l'actuel *RateMyProfessors.com*. Malgré les mises en garde destinées aux élèves et qu'on retrouve sur le site, les atteintes à la réputation et à la vie privée d'un professeur ne sont pas rares.

Malgré la présence de modération, la possibilité de blesser un professeur est très réelle, mais à moins que le commentaire ne soit illégal ou illicite, la liberté d'expression domine. Et pour tenir responsable la personne qui a écrit un message inapproprié, le plus grand obstacle est de la retracer. Sur le site de *RateMyProfessors.com*, on avertit les élèves de la possibilité que leur adresse soit communiquée aux autorités en cas de menaces ou de violence.

2. Quels sont les risques associés aux sites de notation ?

a. La manipulation de l'information et le caractère erroné de celle-ci

Les sites d'évaluation de personnes, de services ou de produits peuvent être manipulés par des gens qui désirent donner une bonne ou une mauvaise note à un produit ou une personne. Par exemple, il est facile pour les amis d'un individu d'aller sur un site d'évaluation de photographies où ce dernier s'est inscrit et de lui attribuer des dizaines de notes parfaites pour augmenter son évaluation. De la même façon, certains sites de commerce électronique étant basés sur la réputation des commerçants, il peut être tentant de publier une évaluation pour soi-même ou pour des amis dans le but d'embellir un profil. Un vendeur qui désire frauder via un site de vente aux enchères pourrait donc se faire attribuer des évaluations positives par ses amis afin d'attirer la confiance des consommateurs.

De plus, les évaluations sur ces sites ne représentent pas toujours fidèlement la satisfaction des gens face à une transaction. Par exemple, sur un site comme eBay, où les cocontractants s'évaluent mutuellement après une transaction, certains peuvent craindre de donner une mauvaise évaluation à la personne avec qui elles ont fait affaire de peur d'en recevoir une en retour par vengeance. Le vendeur d'un article pourrait, suite à la publication d'un commentaire négatif de la part de l'acheteur, publier lui aussi un commentaire mentionnant la mauvaise foi de l'acheteur, même si celui-ci a rempli ses obligations.

Questions à vérifier

- *Est-il possible de soumettre plusieurs évaluations provenant de la même personne ?*
- *Le mécanisme d'évaluation fait-il en sorte qu'une personne peut craindre de subir des représailles suite à une évaluation négative ?*

b. Les atteintes à la réputation et à la vie privée

Il est possible d'entacher la réputation de quelqu'un en évaluant le service ou le produit qu'elle fournit. En effet, le but du service d'évaluation est de noter un service, un produit ou une personne. Chaque évaluation négative atteindra donc nécessairement la réputation de la personne qui fournit le bien ou le service et c'est habituellement l'objectif poursuivi pour éviter que d'autres acheteurs ou vendeurs fassent affaire avec un cocontractant négligent.

Par contre, il faut éviter de faire une évaluation négative qui rapporterait des faits mensongers ou encore des faits véridiques rappelés inutilement dans le seul but de nuire. Par exemple, dire d'un auteur qu'il est un criminel sur un site d'évaluation et de vente de livres peut attenter à sa réputation.

Sur le site *Ratemyprofessors.com*, une liste des choses à faire et à ne pas faire est disponible pour diriger les élèves voulant inscrire un commentaire concernant leurs professeurs[116] :

DOs :

- *Be honest.*
- *Be objective in your assessment of the professor.*
- *Limit your comments to the professor's professional abilities. Do not to get personal.*
- *Proof your comments before submitting. Poor spelling WILL NOT cause your rating to be removed; however, poor spelling may result in your rating being discredited by those who read it.*
- *Leave off your Name, Initials, Pseudo Name, or any sort of identifying mark when posting.*
- *Refer to the Rating Categories to help you better elaborate your comments.*

---

116 « Posting Guidelines », RateMyProfessors.com, en ligne : <http://www.ratemyprofessors.com/ rater_guidelines.jsp> (site consulté le 14 juin 2010).

- *Remember that negative comments that still offer constructive criticism are useful. Comments that bash a professor on a personal level are not.*
- *Submit helpful comments that mention professor's ability to teach and/or communicate effectively, course load, type of course work and course topics.*

DO NOTs :

- *State something as a fact if it is your opinion.*
- *Post a rating if you are not a student or have not taken a class from the professor.*
- *Post ratings for people who do not teach classes at your college or university.*
- *Input false course or section codes for a class that does not exist.*
- *Rate a professor more than once for the same class.*
- *Make references to other comments posted.*
- *Professors : Do not rate yourselves or your colleagues.*[117]

Questions à vérifier

- *Le participant est-il amené à dévoiler des renseignements personnels sur lui-même ou sur une autre personne ?*
- *Est-ce que le site d'évaluation de personnes, de produits ou de services offre une méthode pour dénoncer le contenu inapproprié ?*
- *Est-il possible de soumettre plusieurs évaluations provenant de la même personne ?*

c. La divulgation de renseignements personnels

La divulgation de renseignements personnels sur des sites tels ceux proposant un service de rencontres (adresse de courriel, numéro de téléphone, adresse) peut donner lieu à l'envoi de menaces ou au harcèlement.

Une personne peut également publier une évaluation qui révèle des informations personnelles sur elle-même ou un tiers. La plupart des sites interdisent de mettre en ligne ces informations et les suppriment lorsqu'une telle publication est portée à leur connaissance[118].

Questions à vérifier

- *Le participant est-il amené à dévoiler des renseignements personnels sur lui-même ou sur une autre personne ?*
- *Est-ce qu'il y a présence de modération sur le site ?*

---

117 « Posting Guidelines », RateMyProfessors.com, en ligne : <http://www.ratemyprofessors.com/rater_guidelines.jsp> (site consulté le 14 juin 2010).

118 Sarah COLOMBO, « Trade association proposed to represent rating websites », *Online Journalism Review*, 10 mai 2007, en ligne : <http://www.ojr.org/ojr/stories/070508colombo> (site consulté le 14 juin 2010).

d. L'utilisation non autorisée de l'image

Sur certains sites d'évaluation, il est possible de publier la photographie de la personne évaluée. Cette publication peut être faite avec l'accord de la personne concernée ou sans son consentement, ce qui peut constituer une utilisation non autorisée de son image.

Question à vérifier
• *Est-il possible de publier la photographie d'une personne sur le site d'évaluation ?*

e. La responsabilité pour les informations diffusées

La question de savoir qui est responsable de l'information se retrouvant sur un site d'évaluation de personnes, de produits et de services reste entière. Ces sites se déchargeront habituellement de la responsabilité du contenu publié par les participants, mais s'ils sont avertis qu'un propos illicite se retrouve sur le site, ils ont l'obligation de réagir et de le retirer si le caractère illicite se confirme (art. 22 de la *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1).

Par contre, pour tenir responsable la personne qui a écrit un message inapproprié, le plus grand obstacle est de la retracer. En effet, dans la plupart des cas, les sites d'évaluation ne demandent aucune information permettant d'identifier la personne qui évalue un produit. Certains sites préviennent l'usager que son adresse IP sera enregistrée. Pour retracer une personne qui aurait mis en ligne un commentaire menaçant, par exemple, il faudrait obtenir cette adresse IP enregistrée par le site et l'heure de la publication. Ensuite, il faut vérifier à qui appartenait cette adresse à cette heure précisément auprès du fournisseur d'accès à Internet. Même après ces démarches, il n'est pas garanti que l'identité de la personne soit retracée. Par exemple, sur le site de *RateMyProfessors.com*, on prévient les élèves de la possibilité que leur adresse soit communiquée aux autorités en cas de menaces ou de violence[119].

Questions à vérifier
• *Est-ce qu'il y a des mécanismes de surveillance du contenu sur le site en question ?*
• *Les interventions anonymes sont-elles permises ?*
• *Est-ce que le site Internet sauvegarde des informations personnelles permettant de retracer une personne ? Si oui, le site prévient-il les usagers de cette sauvegarde ?*

119 « Posting Guidelines », RateMyProfessors.com, en ligne : <http://www.ratemyprofessors.com/rater_guidelines.jsp> (site consulté le 14 juin 2010).

3. Comment évaluer ces risques ?

a. L'objet de l'évaluation et les fonctions offertes par le site

Sur les sites d'évaluation, on peut noter des biens, des personnes, des services, etc. Les risques ne sont pas les mêmes, dépendant de l'objet de l'évaluation. Par exemple, un site qui propose d'évaluer les attributs physiques d'une personne risque davantage de poser des problèmes de droit à l'image qu'un site qui permet d'apprécier la qualité de l'histoire d'un livre de poche.

De plus, les fonctions offertes sur le site ont un grand impact sur les risques qui y sont associés. Un site qui offre de laisser un commentaire, en plus d'une évaluation chiffrée, ouvre une porte à des propos diffamants à l'égard d'une personne. Par contre, un site qui n'offre que l'évaluation chiffrée de 1 à 10 présente moins de problèmes, car il ne laisse pas la possibilité de publier des commentaires personnels.

Questions à vérifier
- *Quel type d'évaluation retrouve-t-on sur le site Internet ?*
- *Est-il possible de joindre un commentaire à une évaluation ou est-ce seulement une évaluation chiffrée ?*

b. La présence de modération

Certains sites d'évaluation de personnes, de produits et de services préfèrent mettre en place un mécanisme de modération pour s'assurer que les évaluations des usagers ne comportent pas de contenu inapproprié. Cette modération peut se faire avant que l'évaluation soit publiée ou après.

Lorsque la modération est faite *a priori,* les évaluations soumises ne seront pas immédiatement mises en ligne une fois complétées. Il y aura plutôt un délai de quelques jours avant que l'on puisse les consulter. Cette procédure est utilisée, entre autres, par le site Amazon, qui se réserve un délai de cinq à sept jours avant la publication des évaluations et des commentaires.

La modération peut se faire également *a posteriori*, c'est-à-dire après que l'évaluation soit en ligne. Dans la plupart des cas, les sites qui modèrent avant la publication vont également le faire après puisqu'il est toujours possible qu'un contenu inapproprié ait été publié par erreur. Habituellement, ce type de modération se fait grâce aux utilisateurs du site. Chaque évaluation sera associée à un lien, généralement nommé « *Flag this rating* », invitant à dénoncer le contenu s'il paraît illicite. Lorsqu'un commentaire est signalé, un modérateur du site l'analyse et décide s'il faut le retirer. C'est la procédure utilisée, par exemple, sur le site *RateMyProfessors.com*. Ce site a la particularité de retirer l'évaluation le temps de la révision, en changeant le commentaire par le message « *(Rating under review)* ». Sur ce site, on liste les

commentaires qui seront enlevés, car jugés contraires au bon fonctionnement et à la licéité du site.

COMMENTS THAT CONTAIN THE FOLLOWING WILL BE REMOVED :

- Profanity, name-calling, vulgarity or sexually explicit in nature.
- Derogatory remarks about the professor's religion, ethnicity or race, physical appearance, mental and physical disabilities.
- References to professor's sex life (Including sexual innuendo, sexual orientation or claims that the professor sleeps with students).
- Claims that the professor shows bias for or against a student or specific groups of students.
- Claims that the professor has been or will be fired, suspended from their job, on probation.
- Claims that the professor engages or has previously engaged in illegal activities (drug use, been incarcerated).
- Includes a link/URL to a webpage or website that does not directly pertain to the class.
- Any piece of information including contact info that enables someone to identify a student.
- Any piece of information about the professor that is not available on the school's website and allows someone to contact them outside of school. This also includes remarks about the professor's family and personal life.
- Accusations that the professors are rating themselves or their colleagues.
- Is written in a language other than English ? Unless you attend a French-Canadian school.[120]

D'autres sites prévoient des sanctions pouvant être prises en cas de récidive par les membres ne respectant pas les règles de conduite mises en place.

Question

- *Est-ce que le site d'évaluation est modéré ? Si oui, de quelle façon ? Cela se fait-il avant ou après la publication d'une évaluation ?*

c. Le caractère anonyme ou non des participants

Sur un site où l'anonymat est totalement garanti, la publication de propos susceptibles d'être mensongers est plus facile que sur un site où il faut s'identifier. D'un autre côté, un site exigeant de s'identifier pour publier un commentaire risquerait de diffuser des informations trompeuses ou erronées puisque les gens pourraient se retenir de dire vraiment ce qu'ils savent par crainte de représailles.

Questions à vérifier

- *Est-ce que les participants communiquent dans l'anonymat ?*
- *Est-ce que les participants utilisent des pseudonymes ?*
- *Est-ce qu'il y a des restrictions quant aux personnes pouvant publier un commentaire ?*

120 « Posting Guidelines », RateMyProfessors.com, en ligne : <http://www.ratemyprofessors.com/rater_guidelines.jsp> (site consulté le 14 juin 2010).

d. La possibilité de laisser plusieurs évaluations pour un même produit ou une même personne

Certains sites permettent à un utilisateur de laisser une seule évaluation pour un produit ou une personne. Cela réduit, par exemple, le risque que l'évaluation d'un produit ou d'un service d'une personne soit manipulée par ses amis qui veulent lui donner une bonne note. Cela affecte donc la crédibilité accordée aux propos en ligne. Par exemple, si plusieurs commentaires positifs existent pour un restaurant sur un site où il n'existe aucune limite de commentaires, ces derniers perdront de leur force probante puisqu'on pourra se demander à juste raison s'ils émanent ou non de réels clients témoignant de leur véritable expérience avec l'établissement.

Ce contrôle peut se faire en limitant le nombre de commentaires possibles pour une adresse IP donnée, comme le fait le site *RateMyProfessors.com*. En effet, si plusieurs évaluations sont envoyées par la même adresse IP dans une courte période de temps, les modérateurs supprimeront ces messages.

> ***Question à vérifier***
> - *Est-ce que le site d'évaluation empêche que plusieurs évaluations proviennent de la même personne ?*

4. Quelles sont les précautions à prendre ?

a. Établir des conseils d'écriture pour les évaluations

Pour éviter la mise en ligne de contenu inapproprié, il peut être prudent pour un site d'évaluation de mettre à la disposition des usagers des conseils d'écriture. Ces conseils informent les participants des pratiques tolérées et celles qui ne le sont pas. Lorsque ces conseils se retrouvent déjà sur le site, il est important d'en prendre connaissance pour éviter qu'un commentaire publié soit retiré.

b. Mettre sur pied un processus de vérification du contenu

Que ce soit par les utilisateurs ou par les administrateurs du site, il serait prudent de mettre sur pied une procédure de vérification du contenu. La loi québécoise prévoit que les responsables de sites dans lesquels se retrouvent des documents placés par les usagers n'ont pas l'obligation d'exercer une surveillance.

Mais une procédure de vérification du site par les utilisateurs peut être une bonne alternative. Il s'agit d'inviter les gens à dénoncer un contenu illicite, par une méthode facile offerte par le site. En plus de disposer d'un plus grand nombre de vérificateurs puisque tous les visiteurs peuvent dénoncer un fichier, cette méthode n'engagera pas indûment la responsabilité du site, à moins qu'il ait été averti de l'existence d'un contenu illicite et qu'il n'ait pas agi promptement pour le vérifier.

c. Établir une politique d'utilisation du site

Le site d'évaluation de personnes, de produits ou de services doit établir des règles quant à l'utilisation de son service. Il doit fixer les conditions de la participation d'un internaute au site[121]. Il pourrait, entre autres, interdire les propos à caractère sexuel ainsi que ceux qui propagent un message de racisme ou de violence. Si les conditions d'utilisation ne sont pas respectées, le site peut se réserver le droit de supprimer le commentaire ou de fermer le compte de la personne mal intentionnée.

d. Informer les participants des risques liés à l'usage des sites de notation

Il est important de sensibiliser les usagers aux risques auxquels ils s'exposent en utilisant les sites d'évaluation ou de notation, que ce soit pour la préservation de leurs renseignements personnels ou pour éviter de se voir reconnaître responsable d'une situation.

F. Les sites Wikis

1. Qu'est-ce qu'un site Wiki ?

Un Wiki est « un type particulier de site Web permettant à une communauté de créer et de modifier collectivement un contenu publié en ligne »[122]. Le terme «*Wiki*» est un mot dérivé de l'expression hawaïenne *wikiwiki* qui signifie «vite»[123].

Les Wikis remplissent une multitude de fonctions; ils sont utilisés comme site d'information en ligne, roman ou encore document collaboratif sur un lieu de travail. Contrairement à un blogue, qui est davantage le résultat du travail d'un seul individu, un site Wiki fait appel à la collectivité. Les visiteurs sont appelés à intervenir sur le site en ajoutant ou en corrigeant des informations inexactes ou incomplètes.

Les Wikis sont des sites qui se distinguent par leur aspect collectif et collaboratif. Leur caractéristique fondamentale est que le simple visiteur du site peut en modifier le contenu. Les Wikis n'utilisent pas une hiérarchie formelle, mais sont plutôt structurés de façon horizontale (hyperliens entre les pages du site et avec des pages externes). Ils constituent une des figures exemplaires du phénomène du Web 2.0. Il existe des Wikis

---

121 Anne-Sophie POGGI, « Sites marchands participatifs : 3 règles pour éviter le hors piste », *Le Journal du Net*, 11 septembre 2007, en ligne : <http://www.journaldunet.com/ebusiness/expert/14224/sites-marchands-participatifs---3-regles-pour-eviter-le-hors-piste.shtml> (site consulté le 14 juin 2010).

122 Lucie AUDET, « Wikis, Blogues et Web 2.0, Opportunités et impacts pour la formation à distance », *Le Réseau d'enseignement francophone à distance du Canada (REFAD)*, mars 2010, en ligne : <http://www.refad.ca/nouveau/Wikis_blogues_et_Web_2_0.pdf> (site consulté le 28 juin 2010).

123 Office québécois de la langue française, « site Wiki », en ligne : <http://www.granddictionnaire.com/BTML/FRA/r_Motclef/index1024_1.asp> (site consulté le 29 juin 2010).

publics comme Wikipédia et d'autres privés ou à accès restreint où un mot de passe et un nom d'usager sont nécessaires[124].

Les sites Wikis imposent souvent des règles quant à leur utilisation. En effet, une plus grande liberté d'effectuer une modification de contenu ne signifie pas une absence de contrôle. On interdira généralement le plagiat d'une œuvre protégée ou encore les propos insultants. Certains sites restreignent également les paramètres de modification des articles aux seuls membres enregistrés qui auront fourni leur véritable identité. Pour plus de sécurité, chaque modification est conservée dans une base de données. Si une personne mal intentionnée efface des articles, il sera alors possible de les récupérer. On peut voir l'historique de ces modifications en cliquant sur le lien «Historique» du site Wiki.

Pour créer un site Wiki, il faut tout d'abord posséder un logiciel de gestion de sites Wikis comme MediaWiki[125], TWiki[126] et MoinMoin[127]. Si le site Wiki est déjà créé et que l'on veut apporter certaines modifications, cela ne demande aucun logiciel en particulier; il suffit de se rendre sur la page en question et de cliquer sur le lien « Voir le texte source » ou « Modifier ». En comparaison, la modification d'un site Wiki est un peu plus difficile que la modification d'un blogue. En effet, pour éditer un texte « Wiki », il faut utiliser le langage Wikitexte, qui ressemble à du langage HTML – le langage des pages Web régulières, en version simplifiée. Il faut alors mettre certains mots entre crochet ou ajouter des expressions devant des mots pour faire la mise en forme du texte. Cependant, pour les fonctions de base, comme mettre un mot en caractère accentué, des icônes, semblables à celles qui se retrouvent dans un logiciel de traitement de texte, facilitent le travail[128].

Les articles publiés sur un site Wiki sont habituellement libres de droits, la licence de documentation libre GNU[129] étant généralement utilisée. Une fois en ligne, les utilisateurs ayant les autorisations nécessaires peuvent donc reprendre l'article et le modifier à leur guise. Toute personne connectée à Internet peut agir, sans aucune

---

124 Lucie AUDET, « Wikis, Blogues et Web 2.0, Opportunités et impacts pour la formation à distance », *Le Réseau d'enseignement francophone à distance du Canada (REFAD)*, mars 2010, en ligne : <http://www.refad.ca/nouveau/Wikis_blogues_et_Web_2_0.pdf> (site consulté le 28 juin 2010).

125 « Welcome to MediaWiki.org », MediaWiki, en ligne : <http://www.mediawiki.org/wiki/MediaWiki/> (site consulté le 23 juin 2010).

126 TWiki, en ligne : <http://twiki.org/> (site consulté le 28 juin 2010).

127 MoinMoin, en ligne : <http://moinmo.in/> (site consulté le 28 juin 2010).

128 Sébastien BLONDEEL, *Wikipédia : comprendre et participer*, coll. « Connectez-moi ! », Paris, Éditions Eyrolles, 2006.

129 « GNU Operating System », en ligne: <http://www.gnu.org/copyleft/fdl.html> (site consulté le 23 juin 2010).

formalité d'inscription[130]. Ainsi, tout utilisateur enregistré peut créer un nouvel article, puis tout internaute peut éditer ces articles, en ajoutant, supprimant ou modifiant du contenu.

L'exemple le plus connu d'un site Wiki est sans doute Wikipédia, une encyclopédie en ligne, qui constitue le plus important site Wiki du monde[131]. On y retrouve plus de 950 000 articles en français et plus de sept millions d'articles dans une multitude de langues[132]. Outre la populaire encyclopédie, il existe d'autres Wikis qui comportent souvent, sous une forme ou une autre, un aspect encyclopédique.

a. Qui fait quoi ?

i) Les lecteurs

Les lecteurs sont ceux qui se rendent sur les sites Wikis afin de consulter les informations qui s'y trouvent. Ainsi les utilisateurs se rendront sur Wikipédia pour obtenir de l'information sur un sujet quelconque, iront sur Wikitravels pour découvrir une destination voyage, etc. Le lecteur n'édite pas les informations qu'il lit, il peut le faire, mais il devient à ce moment un acteur actif du monde des Wikis.

ii) Les éditeurs /les Usagers

Les éditeurs sont les acteurs qui participent à la construction de sites Wikis. Ce sont eux qui créent le contenu des pages Web et qui les modifient au fil du temps.

> Tous les rédacteurs des articles de Wikipédia sont bénévoles ; ils constituent une communauté collaborative, sans dirigeant, où les membres coordonnent leurs efforts au sein des projets thématiques et de divers espaces de discussion. Les débats et remarques sur les articles sont bienvenus. Les pages de discussion servent à centraliser les réflexions et les évaluations permettant d'améliorer les articles.[133]

De plus, sur Wikipédia, des informations sur les usagers sont disponibles (comme l'heure, la date et le nombre de modifications) et sont accessibles au public grâce à la page des « contributions de l'usager ». Selon Wikipédia, le compte d'usagers ne sera

---

130 Louise-Marie RIOUX SOUCY, « Wikipédia resserre les rênes », *Le Devoir*, 7 décembre 2005, en ligne : <http://www.ledevoir.com/2005/12/07/97136.html> (site consulté le 23 juin 2010).

131 Wikipédia, en ligne : <http://www.wikipedia.org/> (site consulté le 23 juin 2010).

132 « Bienvenue sur Wikipédia », Wikipédia, en ligne : <http://fr.wikipedia.org/wiki/Wikip%C3%A9dia:Accueil_principal> (site consulté le 23 juin 2010).

133 Wikipédia, en ligne : <http://fr.wikipedia.org/wiki/Wikip%C3%A9dia:Accueil_principal> (site consulté le 29 juin 2010).

jamais supprimé. « La suppression de données spécifiques d'un compte utilisateur est laissée à la discrétion de la politique de suppression du wiki où le compte est actif »[134].

iii) Les administrateurs / les développeurs

De nombreux débats d'idées naissent tous les jours sur Wikipédia, ainsi que des conflits d'autres natures, tels que les enjeux de vie privée ou de propriété intellectuelle. Le site a donc mis en place un système gradué de résolution des conflits : principe de bonne foi, page de discussion, médiation informelle, médiation formelle, arbitrage[135]. Ce système permet de solutionner la plupart des différends sans avoir recours aux tribunaux.

Le site Wikimedia a mis en place un système d'administrateurs qui font un travail d'administration sur les serveurs de Wikimedia[136]. Ce sont eux qui retirent les éléments qui ont été dénoncés comme portant atteinte aux droits ou comme violant les règles des sites Wikis, notamment par rapport au droit d'auteur.

Il peut arriver que les administrateurs de Wikipédia suppriment définitivement certaines parties de l'historique d'un article, dans les cas de diffamation par exemple ou lorsqu'une information privée a été mise en ligne (par exemple un numéro de téléphone). Comme l'historique peut être consulté par tout internaute, la diffamation ou l'atteinte à la vie privée pourrait continuer à causer du dommage si l'historique n'était pas expurgé de son contenu litigieux.

iv) Les hébergeurs

Les hébergeurs sont ceux qui permettent aux sites Wikis de voir le jour. Pensons aux Wikis gratuits qui offrent de l'hébergement: MediaWiki, Wikispaces, PBwiki, wetpaint, Wikia, BluWiki et XWiki.

L'hébergeur ne crée pas de contenus à proprement parler. Il « héberge » le contenu que les usagers créeront dans les pages Web. Cela est d'autant plus vrai avec les pages Wikis où les usagers sont au cœur de la création du matériel disponible.

b. Utilisation des sites wikis en éducation

Les sites Wikis ont plusieurs utilisations possibles en éducation.

---

134 « Information sur les utilisateurs – Politique de confidentialité », Wikimedia Foundation, en ligne : <http://wikimediafoundation.org/wiki/Politique_de_confidentialit%C3%A9#Information_sur_les_utilisateurs> (site consulté le 29 juin 2010).

135 « Wikipedia : Dispute resolution », Wikipédia, en ligne : <http://en.wikipedia.org/wiki/Wikipedia:Dispute_resolution> (site consulté le 22 juin 2010).

136 « System administrators », Wikipédia, en ligne : <http://meta.wikimedia.org/wiki/Developers> (site consulté le 29 juin 2010).

- Contribution à l'élaboration de documents de référence[137]

La contribution à l'élaboration de documents est l'usage le plus courant des Wikis. Le site est alors utilisé pour construire des encyclopédies sur un thème en particulier ou encore des portails de gestion de connaissances de groupes.

Un enseignant du Cégep de Chicoutimi a initié un projet visant à faire travailler ses élèves dans l'ajout de contenu sur Wikipédia[138]. Il explique :

> Dans le cas d'un travail lié à un projet pédagogique sur Wikipédia, les modifications d'articles ou nouveaux articles créés par les étudiants sont accessibles par l'ensemble des francophones de la planète. De plus, les contributions étudiantes sont évaluées par les autres contributeurs et, si elles sont jugées appropriées, demeureront des années en ligne et serviront de base pour les autres wikipédiens qui voudront s'attaquer au sujet traité.

Il décrit ainsi les tâches effectuées par ses élèves dans leur utilisation de Wikipédia à des fins académiques :

> Que ce soit la correction orthographique des articles, la traduction, la mise en page, la catégorisation, la création de liens hypertextes sur certains mots des articles, ou la pose de bandeaux d'avertissements sur des articles incomplets, mal écrits, promotionnels, sans références, violant le copyright ou ne remplissant tout simplement pas les critères d'admissibilité, à peu près tout le monde (et, donc, tous les étudiants) peut y trouver son compte.

Le site Wikimini[139] a été créé pour des enfants et le contenu est mis en ligne par des enfants et des adolescents. Nombre d'articles ont été rédigés par des plus jeunes. Il existe sur le site une section pour les enseignants et les écoles afin que ces derniers intègrent la démarche éducative dans le cheminement scolaire des élèves. Ainsi une classe peut se pencher sur un sujet, effectuer une recherche et ensuite inscrire les informations en ligne.

- La recherche dans les sources des sites Wikis et l'évaluation de leur valeur ou de leur pertinence[140]

---

137 Lucie AUDET, « Wikis, Blogues et Web 2.0, Opportunités et impacts pour la formation à distance », *Le Réseau d'enseignement francophone à distance du Canada (REFAD)*, mars 2010, en ligne : <http://www.refad.ca/nouveau/Wikis_blogues_et_Web_2_0.pdf> (site consulté le 28 juin 2010).

138 Simon VILLENEUVE, « Projet pédagogique sur Wikipédia », *ProfWeb*, 16 février 2009, en ligne : <http://www.profweb.qc.ca/fr/publications/recits/projet-pedagogique-sur-wikipedia/index.html> (site consulté le 28 juin 2010).

139 Wikimini, en ligne : <http://fr.wikimini.org/wiki/Accueil> (site consulté le 28 juin 2010).

140 Lucie AUDET, « Wikis, Blogues et Web 2.0, Opportunités et impacts pour la formation à distance », *Le Réseau d'enseignement francophone à distance du Canada (REFAD)*, mars 2010, en ligne : <http://www.refad.ca/nouveau/Wikis_blogues_et_Web_2_0.pdf> (site consulté le 28 juin 2010).

Les Wikis constituent une source documentaire importante pour les élèves dans la réalisation de leurs travaux. Ils leur permettent aussi d'aiguiser leur sens critique en analysant la pertinence et la qualité des informations trouvées en ligne.

- Élaboration collaborative de documents liés à un travail d'équipe[141]

Les sites tels que Wikipédia permettent de créer des pages d'informations, ou de modifier celles qui existent déjà. Les Wikis peuvent être complètement publics, permettant à n'importe quel internaute d'en modifier le contenu, ou privés, ce qui peut être pratique dans le cas d'un projet d'équipe[142]. Le contenu des wikis peut être sous plusieurs formats : textes, images, vidéo, audio, etc.

Les Wikis offrent de multiples possibilités aux enseignants et à leurs élèves, par exemple :

- Les élèves peuvent annoter directement les documents mis par leur enseignant sur le Wiki (par exemple, un poème ou un extrait de livre)[143].
- Les élèves peuvent collaborer sur des travaux d'équipe[144]. Le Wiki permet aux élèves de toujours travailler sur la version la plus récente du document.
- Les élèves peuvent écrire, réviser et soumettre à leur enseignant leurs travaux scolaires[145]. Ils peuvent même documenter leurs démarches sur le Wiki en publiant leurs sources documentaires au fur et à mesure que leurs recherches avancent. Puisque le Wiki enregistre automatiquement chaque modification faite au document, il est possible de voir son évolution.
- Les élèves peuvent utiliser les Wikis pour compiler des données ou partager les résultats de leurs recherches[146]. Il leur est ainsi possible de retrouver leur travail de n'importe quel endroit où ils ont l'accès à Internet.

---

141 Lucie AUDET, « Wikis, Blogues et Web 2.0, Opportunités et impacts pour la formation à distance », *Le Réseau d'enseignement francophone à distance du Canada (REFAD)*, mars 2010, en ligne : <http://www.refad.ca/nouveau/Wikis_blogues_et_Web_2_0.pdf> (site consulté le 28 juin 2010).

142 « Using Wikis in Education », *Future Changes*, en ligne : <http://www.futurechanges.org/education/> (site consulté le 28 juin 2010).

143 Susan KINZIE, « Blogging Clicks With Colleges, Interactive Web Pages Changing Class Participation », *Washington Post*, 11 mars 2005, en ligne : <http://www.washingtonpost.com/wp-dyn/articles/A25305-2005Mar10.html> (site consulté le 28 juin 2010).

144 « Using Wikis in Education », *Future Changes*, en ligne : <http://www.futurechanges.org/education/> (site consulté le 28 juin 2010).

145 « Using Wikis in Education », *Future Changes*, en ligne : <http://www.futurechanges.org/education/> (site consulté le 28 juin 2010).

146 « Using Wikis in Education », *Future Changes*, en ligne : <http://www.futurechanges.org/education/> (site consulté le 28 juin 2010).

2. Quels sont les risques associés aux sites Wikis ?

En général, les fondateurs d'un site Wiki comptent sur le bon sens et la responsabilité des visiteurs pour réguler le site. Ceux-ci doivent, s'ils trouvent un article faux ou inapproprié, le corriger ou le supprimer. Par contre, il y a parfois des failles dans ce système donc il est important d'examiner les risques que peut engendrer l'utilisation d'un site Wiki.

a. Les informations inexactes ou contrôlées

Le risque que des informations inexactes se retrouvent dans un site Wiki est grand. Dans un site Wiki où les gens collaborent pour écrire un roman, le risque est moins important puisque c'est de la fiction. Par contre, pour prendre l'exemple de Wikipédia, qui met en ligne une encyclopédie modifiable par tous, les individus qui écrivent des articles ne sont pas tous des professionnels du domaine. Certaines personnes peuvent, par malveillance ou encore par ignorance, rapporter des informations inexactes qui se retrouvent sur le site. D'un autre côté, on peut y retrouver de l'information très pertinente écrite par des spécialistes ou des gens très bien renseignés. Il convient donc d'être prudent lorsque nous consultons ce genre de sites Internet.

Un autre risque relié aux sites Wikis est de voir l'information contrôlée par des gens ou compagnies en quête de publicité. Par exemple, Wikipédia peut être modifié par tous et de façon anonyme. Certains articles peuvent être utilisés pour mettre en valeur une compagnie ou une personne, contrevenant ainsi au « *neutral point of view* » préconisé par le site. Les auteurs intéressés à valoriser un article jouissent alors de la crédibilité et de l'apparence de neutralité de Wikipédia.

Compte tenu de la popularité de Wikipédia et de la crédibilité que les internautes lui accordent, il va de soi que les personnalités publiques et les compagnies ont intérêt à vérifier ce que le site affirme à leur sujet. Il peut être tentant de faire modifier ou de modifier soi-même l'article qui nous concerne.

Cette attitude est mal vue sur Wikipédia, mais même le cofondateur Jimmy Wales n'a pu s'empêcher de retoucher quelques données peu flatteuses de sa biographie. Il aurait changé sa propre biographie quelque dix-huit fois au courant de l'année 2005[147].

D'ailleurs, les gens œuvrant en relations publiques seraient fréquemment bloqués par Wikipédia lorsqu'ils tentent de modifier les articles concernant les produits ou l'entreprise qu'ils représentent[148].

---

[147] Marie-Ève MORASSE, « Wikipédia : le fondateur change sa propre bio », *Technaute.ca*, 20 décembre 2005, en ligne : <http://technaute.cyberpresse.ca/nouvelles/200512/20/01-16400-wikipedia-le-fondateur-change-sa-propre-bio.php> (site consulté le 22 juin 2010).

[148] Nancy GOHRING, « Microsoft said to offer payment for Wikipedia edits - *It raises questions on the ethics of a company paying someone to edit entries*», Computer World, 23 janvier 2007, en ligne :

Dans le contexte politique, la possibilité pour quiconque de modifier des articles sur Wikipédia devient un enjeu d'une grande importance. Dans les 24 heures précédant la nomination de Sarah Palin comme colistière de John McCain en août 2008, l'article dédié à la biographie de celle-ci a été modifié quelque 30 fois par un éditeur œuvrant sous le pseudonyme de « Young Trigger ». Cette personne anonyme bonifiait l'image de Palin, indiquant notamment sa forte popularité comme gouverneure, rehaussant ses accomplissements en tant que maire de Wasilla et la qualifiant de politicienne d'une intégrité éblouissante (*eye-popping integrity*)[149].

Questions à vérifier

- *Est-ce que l'information se retrouvant sur le site Wiki est présentée comme étant fiable ou est-ce de la fiction ?*
- *Qui sont les gens participant au site Wiki ? Sont-ils anonymes ou identifiables ?*
- *Quel est le sujet de l'article qui nous intéresse ? Est-ce que l'article est susceptible d'être contrôlé par une personne ou une compagnie ?*

b. Les atteintes à la réputation, la propagande haineuse et les menaces

Le risque d'atteinte à la réputation est grand sur les sites Wiki et l'actualité en déborde d'exemple. En effet, lorsque des articles (comme des biographies) sont rédigés, les auteurs peuvent se tromper sur certaines informations, rappeler inutilement des moments de la vie de quelqu'un sans motif légitime ou alors inventer des faits par rapport à une personne. En effet, la facilité d'écrire ou de modifier un article sur un site Wiki ainsi que la grande diffusion du message illicite peut rendre ce moyen d'expression attrayant.

Il est également possible sur des sites Wikis de faire de la propagande haineuse envers un groupe de la société. Que ce soit par des propos racistes insérés dans un texte ou encore un déni d'événements historiques tel l'Holocauste, il est facile de propager ces messages haineux et punis par la loi sur Internet. Au même titre que pour un blogue, des gens pourraient écrire des menaces ou des propos dénigrants concernant une personne ou un groupe de personnes sur un site Wiki.

Les sites Wikis prohibent la diffusion de contenus diffamatoires ou insultants. Le phénomène y est souvent qualifié de vandalisme virtuel. Toutefois l'interdiction n'est pas toujours respectée.

Par exemple, le site Wikipédia est censé fournir des contenus objectifs (à la différence d'un Wiki d'écriture de roman, par exemple). Or, la grande difficulté est que les

---

<http://www.computerworld.com/s/article/9008842/Microsoft_said_to_offer_payment_for_Wikipedia_edits> (site consulté le 22 juin 2010).

149 Noam COHEN, « Don't Like Palin's Wikipedia Story ? Change It », *The New York Times*, 31 août 2008, en ligne : <http://www.nytimes.com/2008/09/01/technology/01link.html?ex=1378008000&en=2690a3850cb270d0&ei=5124&partner=permalink&exprod=permalink> (site consulté le 22 juin 2010).

contributeurs peuvent agir anonymement, car seule l'adresse IP est conservée et les informations ne sont validées par aucune autorité reconnue. Puisque tout le monde peut intervenir sur Wikipédia et qu'aucun contrôle *a priori* n'est effectué (sauf exceptions), il existe un risque de contenu illicite.

Certains articles rédigés sur Wikipédia s'apparentent aux commentaires publiés sur un blogue public sans contrôle *a priori.* En général, le site Wiki effectuera un contrôle *a posteriori* si une plainte est déposée. Toutefois, le risque demeure que des erreurs majeures et/ou malveillantes demeurent sur le site pour une durée indéterminée.

De nombreuses informations erronées peuvent se retrouver sur les pages de Wikipédia, que ce soit de façon innocente ou mal intentionnée. Le plus souvent, ces erreurs demeurent en ligne pour de très courts laps de temps[150]. Par exemple, le 20 janvier 2009, les sénateurs américains Edward Kennedy et Robert Byrd ont été annoncés comme étant décédés, ce qui s'est avéré être un canular. Ces erreurs sont demeurées respectivement cinq et quatre minutes sur Wikipédia avant d'être corrigées[151].

Dans des cas beaucoup plus exceptionnels, les erreurs demeurent en ligne pour une plus longue période. Cela peut causer des dommages plus importants.

Il peut donc y avoir des problèmes de crédibilité, de vandalisme et de diffamation sur un site encyclopédique de référence dont les contenus sont générés par les usagers. Wikipédia a d'ailleurs resserré ses normes de création de contenus, obligeant les créateurs de nouveaux articles à s'enregistrer[152]. Cette mesure a cependant été considérée par certains comme insuffisante ou inutile.[153] En effet, l'enregistrement d'un compte sur Wikipédia ne demande pas de fournir une adresse de courriel valide - on ne garantit donc pas la responsabilité de l'éditeur, et les modifications pouvant toujours être effectuées par n'importe quel internaute.

---

150 Voir par exemple l'étude menée en 2007 concernant les articles portant sur les sénateurs américains : Gregory KOHS, « Wikipedia Vandalism Study – US Senators », *Wikipedia Review*, 5 octobre 2008, en ligne : <http://wikipediareview.com/blog/20081005/wikipedia-vandalism-study-us-senators/> (site consulté le 22 juin 2010).

151 Ben PERSHING, « Kennedy, Byrd the Latest Victims of Wikipédia Errors », *The Washington Post*, 21 janvier 2009, en ligne : <http://voices.washingtonpost.com/capitol-briefing/2009/01/kennedy_the_latest_victim_of_w.html> (site consulté le 22 juin 2010).

152 Louise-Maude RIOUX SOUCY, « Wikipédia resserre les rênes », *Le Devoir*, 7 décembre 2005, en ligne : <http://www.ledevoir.com/2005/12/07/97136.html> (site consulté le 22 juin 2010).

153 Voir Anita RAMASASTRY, « Is an online Encyclopedia, such as Wikipedia, Immune from Libel suits ? », *FindLaw*, 12 décembre 2005, en ligne : <http://writ.news.findlaw.com/ramasastry/20051212.html> (site consulté le 22 juin 2010).

Questions à vérifier
- *Est-ce que l'article contient des informations sur la vie de quelqu'un ?*
- *Est-ce qu'il y a vérification, par les administrateurs du site, du contenu qui est publié ?*

c. Les contenus ne convenant pas aux enfants

De l'information ou des images à caractère pornographique peuvent se retrouver sur des sites Wikis. En effet, puisqu'on peut ajouter du contenu à notre guise, certains peuvent faire des modifications non appropriées, par exemple mettre en ligne des photographies obscènes. Il est donc possible de retrouver de telles images dans un article qui peut être anodin au premier abord.

De plus, certains sites Wikis ont comme finalité de présenter du contenu à caractère pornographique, par exemple des histoires auxquelles plusieurs personnes peuvent collaborer. Ces pages sont plus faciles à repérer puisqu'elles sont affichées comme telles. Les chances d'y être exposé involontairement sont donc plus faibles.

Ce matériel ne convient généralement pas aux enfants, mais il n'est pas illicite. Par contre, nous pouvons retrouver sur un site Wiki du contenu illégal, qui peut prendre la forme de matériel obscène, de bestialité ou encore de pornographie juvénile.

Question à vérifier :
- *Quel est le sujet du site Wiki en question ? Est-ce que le sujet convient au public qui est visé ?*

d. Les atteintes au droit d'auteur et l'utilisation non autorisée de l'image

Lorsque des photographies sont présentes sur un site, cela peut constituer une atteinte au droit à l'image si la personne représentée n'a pas autorisé sa publication. C'est le cas si un site Wiki présente la biographie d'une personne et qu'on y insère sa photographie sans sa permission.

De plus, le participant au site Wiki peut emprunter des oeuvres que l'on retrouve sur d'autres sites Internet ou ailleurs. Cet emprunt peut se faire pour les images mais aussi pour toutes autres œuvres, que ce soit des textes, des chansons, etc. soulevant alors des questions quant au droit d'auteur. En effet, pour publier une œuvre dont on ne détient pas les droits, il faut obtenir la permission de celui qui détient ces droits en vertu de la *Loi sur le droit d'auteur*.

Lorsqu'on établit des liens hypertextes, il faut également s'assurer de respecter le droit d'auteur. Des techniques consistant à reproduire le site à l'intérieur du site Wiki (*framing*) ou encore à copier la banque de liens hypertextes d'un autre site peuvent s'avérer risquées.

Les articles publiés sur Wikipédia sont diffusés sous licence « Creative Commons paternité partage à l'identique », et peuvent donc être copiés, redistribués, modifiés et même commercialisés à certaines conditions de façon mondiale, perpétuelle et sans redevance[154]. Wikipédia condamne les atteintes au droit d'auteur, tout en reconnaissant que la distinction légale entre *copyright* et *fair use* peut être assez complexe[155].

> ***Questions à vérifier***
> - *Est-ce que les articles du site Wiki contiennent des œuvres ou parties d'œuvres qui sont protégées par la Loi sur le droit d'auteur ?*
> - *Est-ce que le participant détient les autorisations nécessaires pour publier tout ce qui se trouve sur celui-ci ?*

e. La responsabilité pour les informations diffusées

Les sites Wiki sont habituellement dans la position d'un hébergeur et n'ont pas à ce titre de responsabilité pour le contenu publié par les participants. Mais s'ils sont avertis qu'un propos illicite se retrouve sur le site, ils ont l'obligation d'effectuer les vérifications appropriées et de le retirer si c'est nécessaire.

La situation se corse si l'on veut retenir la responsabilité d'un auteur d'un article puisqu'il y a en général plusieurs auteurs qui y ont coopéré. La personne qui a inséré le propos fautif dans l'article sera responsable. La question de savoir si la dernière personne qui aurait modifié un article même si elle a seulement corrigé certaines fautes grammaticales est plus délicate. Mais il paraît certain que si un article comportant un contenu illicite se retrouve sur un site Wiki et que l'auteur est la seule personne qui y a contribué, il en sera responsable.

> ***Question à vérifier :***
> - *Est-ce qu'il y a un ou plusieurs auteurs à l'article en question ?*

f. L'utilisation des sites wikis à des fins judiciaires

L'information mise en ligne sur Wikipédia n'étant pas constante quant à sa fiabilité, tant les parties que les juges doivent user de discernement quant aux éléments de preuve qui proviennent de cette encyclopédie. Dans certains cas, la preuve provenant de sites Wikis a été considérée acceptable, alors que dans d'autres, elle a été rejetée. Les enquêtes « maison » effectuées sur Google ou Wikipédia par les membres d'un jury afin de « bonifier » la preuve ou de se faire une opinion sur une situation ou sur une

---

154 « Wikipedia : Copyrights », Wikipédia, en ligne : <http://en.wikipedia.org/wiki/Wikipedia: Copyrights> (site consulté le 22 juin 2010).

155 « Wikipedia : List of Policies », Wikipédia, en ligne : <http://en.wikipedia.org/wiki/ Wikipedia_policy#Legal_and_copyright> (site consulté le 22 juin 2010).

personne, témoin ou accusé sont problématiques. Ces pratiques, difficilement contrôlables, affectent nécessairement l'administration de la justice[156].

Dans *R. c. Cianfagna*[157]*,* le tribunal constate que Wikipédia « ne peut pas (encore) être qualifiée d'encyclopédie ». Il ne peut donc être présumé que Wikipédia constitue une source accessible et fiable. Si les caractères d'accessibilité et de fiabilité ne peuvent pas être présumés, ils pourraient par contre être prouvés. Wikipédia constituerait alors une source sur laquelle pourrait se baser un juge pour prendre connaissance d'office d'un fait. Car le tribunal convient que si Wikipédia, dans sa globalité, ne constitue pas une source fiable, certains de ses articles peuvent être fiables.

3. Comment évaluer ces risques ?

L'ampleur du risque auquel on s'expose en naviguant sur des sites Wikis ou en y participant varie selon ces facteurs : l'accessibilité au site Wiki, le sujet du site, ainsi que le caractère anonyme ou non des participants.

a. L'accessibilité au site Wiki

Il est certain qu'un site Wiki disponible seulement au sein d'une entreprise afin que des employés collaborent à un projet est moins risqué qu'un site se retrouvant sur Internet. En effet, un plus grand contrôle peut être exercé sur un site disponible uniquement par exemple, sur un intranet, puisque les personnes qui y ont accès sont identifiées et identifiables.

En revanche, un site accessible au grand public et qui peut être modifié par tous les visiteurs risque davantage d'être victime de sabotage par des personnes qui sont mal intentionnées. De plus, cette grande accessibilité fait en sorte que les dommages seront plus grands si, par exemple, des propos diffamatoires y sont publiés.

Question
- *Le site est-il accessible par Internet ou limité à un groupe d'usagers comme un intranet ?*

b. Le contenu du site Wiki

Comme pour les pages Web, certains types de contenus ou d'activités sur un site Wiki sont plus problématiques que d'autres. Les articles portant sur des sujets qui soulèvent des points de vue différents risquent d'être moins impartiaux que des articles dont le

---

156 John SCHWARTZ, « As Jurors Turn to Web, Mistrials are Popping Up », *The New York Times*, 17 mars 2009, en ligne: <http://www.nytimes.com/2009/03/18/us/18juries.html> (site consulté le 22 juin 2010).

157 *R. c. Cianfagna*, Cour municipale de Montréal, 2007 CanLII 25904 (QC C.M.), 28 juin 2007, <http://www.iijcan.org/fr/qc/qccm/doc/2007/2007canlii25904/2007canlii25904.html>.

contenu est par définition neutre. Par exemple, une personne peut avoir intérêt à prendre le contrôle d'un article qui porte sur une compagnie pour le rendre davantage favorable à l'entreprise. Par contre, il paraît moins probable qu'un individu falsifie un article portant sur des sortes de fleurs ou encore sur les oiseaux puisque le sujet est neutre.

La nature même de l'article peut influencer les risques. Il peut être risqué d'écrire la biographie d'une personne à son insu puisqu'il est possible que l'on rédige des propos faux ou diffamants. Par contre, un tel risque est moindre lorsqu'on écrit un article scientifique.

Questions à vérifier

- *Quel est le sujet de l'article en question ?*
- *Est-ce que la nature de l'article comporte des risques inhérents ?*

c. Le caractère anonyme ou non des participants

Certains sites Wikis autorisent des auteurs anonymes à publier des articles ou des modifications. D'autres exigeront certains renseignements, comme une adresse de courriel valide ou un pseudonyme, afin de publier du contenu. En exigeant certains renseignements permettant d'identifier l'auteur, on diminue les risques étant donné que les participants peuvent craindre de se faire identifier. De plus, certains sites sont plus exigeants en autorisant uniquement les membres à faire des modifications.

Questions à vérifier

- *Est-ce que les participants communiquent dans l'anonymat ?*
- *Est-ce que les participants utilisent des pseudonymes ?*
- *Est-ce qu'il y a des restrictions quant aux personnes pouvant publier un article ?*

4. Quelles sont les précautions à prendre ?

a. Établir une politique d'utilisation du site Wiki

Il serait prudent pour un site Wiki de mettre en place une politique d'utilisation des services offerts. Celle-ci informerait des usages acceptés et du contenu prohibé. Par exemple, un site Wiki pourrait prévoir qu'un contenu diffamatoire, à caractère pornographique ou encore menaçant, est interdit, qu'il est impératif de respecter le droit d'auteur en rédigeant un article... Si ces conditions ne sont pas respectées, le site peut se réserver le droit de supprimer le contenu inapproprié ou encore il pourrait bloquer le compte d'usager d'une personne qui pose des actes malveillants.

La politique d'utilisation du site Wiki devrait également prévoir que les contributeurs au site sont les seuls responsables du contenu qu'ils publient puisque le service offert se limite à héberger de l'information. Un tel avertissement peut être dissuadant pour une personne ayant l'intention de publier un contenu inapproprié. De plus, on peut préciser,

si c'est le cas, que les administrateurs du site ne participent aucunement à la création du site. Une telle affirmation, dans le cadre d'un recours judiciaire, peut être utile pour établir la ligne de démarcation entre les personnes responsables et celles qui ne le sont pas.

b. Informer les gens des risques inhérents à l'utilisation d'un site Wiki

Il est important de sensibiliser les gens aux risques auxquels ils s'exposent en utilisant les sites Wikis. Les mises en garde peuvent porter sur plusieurs éléments, comme l'obligation de respecter le droit d'auteur ou encore la nécessité de bien se renseigner sur un sujet avant de se fier à une ressource Wiki. Ces avertissements sont très utiles, en particulier lorsqu'on vise un public comme les enfants.

c. Mettre en place une procédure afin de revoir le matériel placé sur le site Wiki pour vérifier sa conformité au droit d'auteur et à d'autres droits

Certains proposent de mettre en place une procédure pour vérifier les informations qui sont déjà publiées sur le site Wiki ou qui vont l'être, dans le but de vérifier leur conformité à la loi. Une telle procédure, même si elle est faite de bonne foi, peut entraîner la responsabilité des administrateurs si un contenu inapproprié est publié, puisqu'ils ont le contrôle de l'information comme un éditeur.

d. Mettre en place une procédure pour répondre aux préoccupations ou plaintes concernant le matériel placé sur le site

Il serait préférable pour un site Wiki de prévoir une procédure simple et efficace pour recevoir les plaintes à l'égard du contenu du site. En effet, une telle méthode est avantageuse autant pour le plaignant que pour les administrateurs du site puisque les recours devant les tribunaux ne sont pas toujours les plus efficaces. La procédure judiciaire peut être longue et coûteuse, et le matériel inapproprié peut rester longtemps sur le site avant qu'un jugement ne soit prononcé. Une procédure à l'interne est donc une bonne alternative. Par exemple, le site peut prévoir que si une information sur le site semble inappropriée, on peut déposer une plainte à un groupe de vérification du site qui jugera si le contenu doit être retiré ou non.

e. Établir des règles de conduite

Avec l'usage, les collaborateurs aux sites Wikis ont développé certaines règles de conduite que chaque personne doit adopter lorsqu'elle participe à un tel site. Ces conventions peuvent être déroutantes pour un débutant dans le domaine puisqu'elles ne sont pas toujours écrites. C'est pourquoi il est préférable de les consigner par écrit lorsqu'un site Wiki est mis en ligne, afin d'en favoriser leur respect. On peut prévoir, par exemple, la nécessité pour les personnes de réviser le contenu avant de publier un article ou encore de décrire les modifications faites sur la page, dans le but de conserver une trace de ce qui a été fait.

G. Les flux RSS

1. Qu'est-ce qu'un flux RSS ?



Un flux RSS (se dit aussi fil RSS) désigne un format utilisé pour publier du contenu web régulièrement mis à jour. RSS est l'abréviation de *Real Simple Syndication*. La syndication de contenu (ou agrégation de contenu) est le fait de rendre un texte (incluant nom de l'auteur, photo, titre et date) indépendant de la structure du site web principal. Ainsi, celui qui désire publier un nouveau message n'a pas à mettre à jour sa page web à chaque entrée. Un site d'actualité utilise les flux RSS pour ses différents sujets (Politique, sport, art… etc.). Une compagnie de produits et services utilise le flux RSS pour annoncer ses nouveaux produits. Le flux ressemble à une page web contenant toutes les nouvelles en ordre chronologique.

Pour l'usager, un agrégateur de contenu (un logiciel comme un navigateur web ou une application en ligne comme Google Reader) permet de rassembler tous les flux et de les gérer. Pour reprendre notre exemple du site d'actualité, l'usager peut recevoir dans son agrégateur les derniers billets de Cyberpresse de la section « Politique ». L'usager n'a plus besoin de naviguer sur les sites pour retrouver ses nouvelles. Les nouvelles viennent à lui. En plus de pouvoir être intégré dans un agrégateur RSS, le flux RSS peut faire l'objet d'incorporation («embedding»), ce qui signifie que n'importe qui peut ajouter le flux de nouvelles dans son site. Par exemple, le webmestre d'un site de sport peut intégrer le flux de nouvelles du site d'une équipe sportive à son propre site.



Au plan technique, RSS et Atom sont deux langages informatiques différents permettant la syndication de contenu. Ils se confondent puisque les sites web utilisent le même logo indépendamment du langage utilisé. Dans tous les cas, le contenu d'un flux RSS est plutôt limité. Il se limite à du contenu texte simple. Toutefois, le standard Atom permet d'ajouter des liens vers des documents photo, audio ou vidéo.

a. Qui fait quoi ?

i) L'usager ou le lecteur

L'usager est la personne physique qui consulte le contenu des flux RSS. Généralement, l'usager gère ses flux par un agrégateur qui lui permet de trier, de classer et de lire un résumé (« chapeau ») des articles d'actualité. Si le chapeau de l'article l'intéresse, l'usager clique sur le lien et est redirigé vers le site Web où l'article est publié en entier. Il est très envisageable que des élèves se constituent des pages Web personnelles ou des blogues. Dans ce cas, ils peuvent avoir envie d'y relayer des flux RSS qui sont susceptibles d'intéresser les visiteurs de leur page. Cela dit, il convient de rappeler que n'importe qui peut générer un flux RSS, et que ces flux ne relèvent pas nécessairement du bon goût.

ii) L'éditeur du contenu

L'éditeur de contenu est la personne qui publie l'article qui sera contenu dans le flux RSS. Les éditeurs de contenus sont multiples. Par exemple, il est possible de s'abonner au flux RSS de Conan O'Brien, un humoriste américain qui publie sur Twitter. À l'opposé, l'Université de Montréal a aussi un fil RSS pour présenter ses plus récents articles. Le flux RSS est donc utilisé par plusieurs sur Internet, et ce, pour des fins bien diverses. Il y existe donc une myriade d'éditeurs de contenus.

iii) Le développeur du site

Le développeur est la personne qui crée, maintient et actualise un site Web. Il arrive de plus en plus que les développeurs utilisent la technique de l'incorporation (*embedding)* pour insérer des flux RSS dans leur propre site ou blogue. Il peut agencer les flux et les répertorier pour les mettre à la disposition de ses visiteurs. De son point de vue, les flux RSS sont des contenus automatisés, car ils se mettent à jour automatiquement. Les sites qui répertorient des contenus automatisés traitant d'un thème commun portent le nom de *mashups* (applications composites).

Lorsque le développeur utilise la technique de l'incorporation (*embedding)*, il relaye le flux RSS. La technique de l'incorporation est très simple et ne requiert pas de connaissances particulièrement poussées pour l'intégrer à un site ou à un blogue. Le développeur de site peut être le site d'une institution scolaire, mais aussi, à l'opposé, celui d'un individu.

b. Utilisation dans le domaine de l'éducation

Les flux RSS servent principalement à suivre l'actualité. Pour un travail donné, un enseignant peut décider de créer un blogue sur lequel s'affichent les flux RSS de sites reliés au sujet.

L'institution scolaire peut utiliser les flux RSS sur son site web pour relayer, par exemple, des lois en matière d'éducation, des actualités d'un chroniqueur en particulier, les actualités municipales, etc. Elle peut aussi créer son propre flux RSS pour afficher l'actualité de l'institution, le calendrier des activités, etc.

2. Quels sont les risques associés à un flux RSS ?

La création de son propre flux RSS emporte les mêmes risques que n'importe quelle publication sur Internet. À l'instar des autres applications supposant la diffusion d'informations comme le blogue, la page Web personnelle, l'espace personnel sur un réseau social, l'éditeur du contenu est responsable des propos qu'il diffuse. Mais le flux RSS comporte un risque particulier : celui qui découle de l'utilisation d'un flux publié par un tiers.

a. Engager sa responsabilité pour le contenu du flux RSS publié par un tiers

Un webmestre qui n'est pas l'auteur d'un document litigieux relayé par un fil RSS mais qui fait le choix de le publier à l'intérieur d'un agencement particulier sur son site pourrait avoir à répondre du contenu qui se trouverait ainsi diffusé même s'il est généré automatiquement. Il en irait ainsi également s'il connaît le caractère illicite des messages qu'il relaie par le truchement d'un fil RSS rendu disponible sur son site.

L'institution scolaire peut relayer les flux RSS de ses élèves. Les élèves peuvent générer des flux RSS via leurs pages Twitter/MySpace ou leurs blogues. Si l'élève rédige des propos médisants au sujet d'une autre personne, ses propos seront alors disponibles à un bien plus grand lectorat. L'institution risque alors d'être tenue responsable envers la personne victime des propos médisants.

Dans l'hypothèse où l'institution génère son propre flux RSS, elle doit agir avec diligence, au même titre que tout autre contenu publié sur sa page Web.

3. Comment évaluer ces risques ?

a. Le public cible du site propulsé par le développeur

Un site qui s'adresse à un large public présente nécessairement plus de risques qu'un site lu par seulement quelques personnes. À qui s'adresse le site ? Le public cible joue un rôle important. Il suffit de prendre pour exemple le site d'une commission scolaire. Le site s'adresse aux contribuables et aux parents des élèves. Un propos médisant n'aura certainement pas le même impact que s'il était uniquement publié sur la page Twitter / Facebook destinée aux quelques amis de l'élève.

b. La place et l'importance attribuées au flux RSS

La place du flux RSS sur un site peut jouer un rôle pour déterminer si le développeur est éditeur ou non. Prenons l'exemple d'un flux RSS disponible sur la page d'accueil du site, et dont le site est construit autour de ce flux RSS. Dans un deuxième cas de figure, le flux RSS se situe dans une section discrète du site intitulée « Partenaires ». Dans le premier cas, il est plus vraisemblable qu'on attribue des fonctions éditoriales au développeur du site. Dans le deuxième cas, le développeur risque moins d'être assimilé à un éditeur, mais pourrait tout de même être tenu responsable pour le contenu illicite dont il a eu connaissance.

4. Quelles sont les précautions à prendre ?

a. Vérifier le site régulièrement

L'une des façons pour le développeur d'éviter d'engager sa responsabilité est de retirer promptement le contenu dès qu'il a connaissance de son caractère illicite. Pour ce faire, le développeur peut visiter régulièrement son site et prendre connaissance des titres, chapeaux et images qui sont relayés via les flux RSS. Dès qu'un contenu possiblement illicite apparaît, le développeur peut se désabonner du flux RSS. Ainsi, il minimise ses risques de partager la responsabilité avec l'éditeur du contenu.

b. Ne relayer que des sites crédibles

Il existe sur Internet une abondance de flux RSS. Lorsque vient le temps de créer une page Web ou un site institutionnel, il convient de ne relayer que des sites dont on peut attester de la crédibilité.

H. La baladodiffusion

1. Qu'est-ce que la baladodiffusion ?

Le mot « podcast » résulte de la combinaison des mots « iPod » (le lecteur MP3 d'Apple) et « broadcast »[158]. Ce type de fichier est appelé « balado »[159] selon l'Office québécois de la langue française.

Les balados sont des dossiers médias numériques qui peuvent être téléchargés sur des ordinateurs et transférés sur un lecteur multimédia portatif. On peut accéder aux balados de plusieurs façons: par un lien RSS (Really Simple Syndication) accessible de la

---

158 Kathleen Elliott VINSON, « What's on Your Playlist ? The Power of Podcasts as a Pedagogical Tool » (2009), 09 *Legal Studies Research Paper Series*, en ligne: <http://ssrn.com/abstract=1337737> (site consulté le 17 juillet 2010).

159 OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Balado », 2006, en ligne : <http://www.grand dictionnaire.com/BTML/FRA/r_Motclef/fiche.asp> (site consulté le 17 juillet 2010).

plupart des navigateurs Internet, par le magasin en ligne iTunes ou alors via d'autres programmes mettant en ligne des balados.

Malgré les origines de son nom, il n'est pas nécessaire de posséder un iPod ou un MP3 pour écouter un balado. On peut télécharger le fichier balado directement du navigateur ou alors il est possible de s'abonner à un balado[160].

Le modèle de syndication RSS permet à l'usager de recevoir des mises à jour automatiques lorsque de nouveaux balados sont disponibles pour le téléchargement. Une fois entrés les paramètres préférés de l'usager quant aux balados, ceux-ci seront automatiquement téléchargés sur son ordinateur[161]. Par exemple, un usager possédant iTunes (le logiciel de musique d'Apple) se rend sur le *iTunes Store* où des centaines de balados sont à sa disposition. Il peut alors choisir ceux qu'il souhaite télécharger dans son ordinateur. Il peut aussi décider de s'abonner – gratuitement ou non – aux balados qu'il aime et ces derniers seront automatiquement téléchargés sur son ordinateur à chaque fois qu'une nouvelle mise à jour (ou épisode) sera disponible.

L'hôte ou l'auteur du fichier balado est appelé baladodiffuseur[162]. La création de balados est simple; cela ne demande pas la technologie d'un studio d'enregistrement professionnel. En effet, un microphone ou un téléphone cellulaire équipé des programmes nécessaires permettent tous deux l'enregistrement de balados. Même si la baladodiffusion a au départ été créée pour diffuser du contenu audio sur Internet, la technologie permet aussi d'avoir accès à des fichiers sous forme de vidéos[163].

La durée d'un balado varie de quelques secondes à plusieurs heures. Certains balados sont gratuits, alors que d'autres ne sont disponibles que moyennant le paiement d'un abonnement.

L'objectif initial de la baladodiffusion était de rendre disponibles les programmes de type radios, et cela demeure à ce jour l'usage le plus répandu[164]. Un balado peut être constitué de fichiers audio ou vidéo d'émissions déjà diffusées ou de programmation

---

160 Kathleen Elliott VINSON, « What's on Your Playlist ? The Power of Podcasts as a Pedagogical Tool », (2009), *Legal Studies Research Paper Series*, en ligne : <http://ssrn.com/abstract=1337737> (site consulté le 17 juillet 2010).

161 Erin M. JACOBSON, « Podcasting 201 : Copyright Infringement Issues when Using Third-party Material in Podcasts », (2008) 26-1 *The Entertainment and Sports Lawyer* 7.

162 OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Baladodiffuseur », 2006, en ligne : <http://www.granddictionnaire.com/BTML/FRA/r_Motclef/fiche.asp> (site consulté le 17 juillet 2010).

163 Holly Beth BILLINGTON, « The Podcasting Explosion : US and International Law Implications », (2006) 18-11 *Intel. Prop. & Tech. L. J.* 5.

164 Gavin SUTTER et Johanna GIBSON, « Podcasts and the Law », (2007) *JISC legal information*.

originale créée spécialement pour la diffusion en ligne[165] comme des conférences, des horoscopes ou des radios indépendantes diffusant sous forme de balados.

Par exemple, un marché important s'est développé au sein de l'industrie du voyage et du tourisme. Ainsi, plusieurs hôtels offrent la possibilité d'utiliser des lecteurs audio portatifs pour visiter une ville donnée au lieu des guides de voyage traditionnels. Les balados sont également utilisés en politique. Le département d'État publiait sous forme de balado les discours de la secrétaire d'État Condoleezza Rice. Le service de police de la ville de New York rend disponible en baladodiffusion des conseils de sécurité ainsi que des communiqués de presse[166]. La radio de Radio-Canada offre aussi des émissions en ligne gratuitement en baladodiffusion et le Planétarium de Montréal, des capsules sur l'astronomie. La plupart des sites de baladodiffusion disponibles au Québec sont accessibles à < http://quebecbalado.com/ >.

a. Qui fait quoi ?

i) L'agrégateur

Les balados peuvent être automatiquement téléchargés selon les préférences de l'usager au moyen d'un logiciel d'agrégation – appelé agrégateur, ou tout autre service de distribution Internet comme le protocole RSS (Really Simple Syndication) . En fait, un agrégateur (de l'anglais *aggregator*) est un logiciel qui permet de suivre plusieurs fils de syndication (RSS) simultanément[167]. Par extension, l'entité qui a la maîtrise du logiciel d'agrégation à l'égard d'un ensemble de balados est l'agrégateur

L'usager n'a donc pas besoin de visiter tous les sites pour savoir s'il y a eu changement au niveau des fichiers balados disponibles puisqu'il obtient l'information automatiquement.

ii) L'hébergeur / l'éditeur

L'éditeur est l'entité qui exerce un contrôle effectif sur la sélection des contenus de même que sur leur organisation, soit suivant une grille chronologique, dans les cas d'émissions télévisées, soit selon un catalogue, dans le cas de services de médias audiovisuels à la demande. Le balado mis en ligne par l'éditeur peut être sa création ou celle d'un tiers, mais il sera dans les deux cas responsable du contenu.

---

165 Holly Beth BILLINGTON, « The Podcasting Explosion : US and International Law Implications », (2006) 18-11 *Intel. Prop. & Tech. L. J.* 5.

166 Holly Beth BILLINGTON, « The Podcasting Explosion: US and International Law Implications », (2006) 18-11 *Intel. Prop. & Tech. L. J.* 5.

167 Wikibena, « Baladodiffusion », en ligne : <https://wiki.umontreal.ca/display/BENA/Utiliser+la+baladodiffusion#Utiliserlabaladodiffusion7.4%C3%89tapeIVRendrevotrebaladoreconnaissableentretous> (site consulté le 20 juillet 2010).

L'auteur du balado, qu'on appelle « podcaster » en anglais, se nomme baladodiffuseur ou baladiffuseur en français[168]. Il crée le fichier balado pour le rendre disponible en ligne. Il est le diffuseur, « qui, par l'entremise d'un abonnement à des fils de syndication, diffuse sur Internet des balados audio ou vidéo, téléchargés automatiquement à l'aide d'un logiciel agrégateur et destinés à être transféré sur un baladeur numérique ou sur un ordinateur pour une écoute ou un visionnement ultérieurs »[169].

Si un site ne fait qu'héberger le contenu des balados sans participer à leur création ou à la décision de diffuser, alors il sera, selon toute probabilité, considéré comme un hébergeur.

iii) L'usager

L'usager est l'acteur central de la baladodiffusion. En effet, le fichier balado est créé pour que celui-ci puisse l'écouter. Lorsque l'usager identifie un balado intéressant, il a trois possibilités: il peut en faire une lecture en transit (en streaming) sans télécharger le fichier, il peut télécharger le fichier balado sans aucune application– ce qui peut être possible sur certains sites– ou finalement il peut le télécharger par le biais d'une application telle *Juice, iTunes, Netvibes*, puis le transférer sur son baladeur[170].

L'usager peut également choisir de s'abonner aux fichiers balados qui l'intéressent. Il recevra alors automatiquement dans son agrégateur chaque mise à jour du fichier balado qui l'intéresse. L'usager pourra alors les écouter sur son ordinateur ou son lecteur MP3[171].

L'auteur des balados met les fichiers en ligne et c'est alors « aux auditeurs que revient le rôle de gérer une liste de lecture avec leurs différents abonnements. Le téléchargement des fichiers est alors automatisé et issu des multiples sources qu'ils ont choisies. En d'autres termes, c'est l'auditoire qui choisit des baladodiffuseurs et les mises à jour des nouveaux balados seront automatiques dans leur agrégateur »[172].

---

168 OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Baladodiffuseur », (2006), en ligne : <http://www.granddictionnaire.com/BTML/FRE/r_Motclef/fiche.asp> (site consulté le 17 juillet 2010).

169 Wikibena, « Baladodiffusion », en ligne : <https://wiki.umontreal.ca/display/BENA/Utiliser+la+baladodiffusion#Utiliserlabaladodiffusion7.4%C3%89tapeIVRendrevotrebaladoreconnaissableentretous> (site consulté le 20 juillet 2010).

170 Anne-Sophie JOUANNON, « Les enjeux juridiques du podcasting », (2008) *Mémoire de master Université de Versailles, St-Quentin-en-Yvelines*.

171 Anne-Sophie JOUANNON, « Les enjeux juridiques du podcasting », (2008) *Mémoire de master Université de Versailles, St-Quentin-en-Yvelines*.

172 Wikibena, « Baladodiffusion », en ligne : <https://wiki.umontreal.ca/display/BENA/Utiliser+la+baladodiffusion#Utiliserlabaladodiffusion7.4%C3%89tapeIVRendrevotrebaladoreconnaissableentretous> (site consulté le 20 juillet 2010).

b. Utilisation de la baladodiffusion en éducation

Les étudiants peuvent écouter les fichiers balados n'importe où et n'importe quand, selon leur goût et sans les contraintes de temps et d'espace de la salle de classe. Par exemple, les étudiants peuvent écouter leurs balados et garder leurs yeux et mains libres pour d'autres tâches ou d'autres activités. Les fichiers balados constituent également une excellente alternative pour tenir compte des différents styles d'apprentissage des étudiants[173].

Les fichiers balados sont des fichiers enregistrés, ayant l'avantage de pouvoir être réécoutés. Ils peuvent être utilisés comme outil de révision ou d'apprentissage. Les enseignants peuvent donc enregistrer des cours, des leçons ou n'importe quel autre contenu afin de permettre à leurs élèves de les télécharger.

Le site de l'Université de Montréal suggère les utilisations suivantes pour les fichiers balados[174] :

> - ***Enregistrement d'un cours en classe***
>
> *L'enregistrement d'un cours en classe peut être dans un format audio ou vidéo.*
>
> - ***Accès à des modules préparatoires avant le cours***
>
> *Avant le prochain cours, les étudiants peuvent se préparer en écoutant une conférence préenregistrée, une lecture préparatoire à une discussion, une mise en contexte pour un atelier ou une étude de cas. Ces différents exemples de modules peuvent faciliter l'interaction entre les étudiants, avoir une meilleure préparation pour le cours, faciliter les échanges entre les étudiants et l'enseignant ou se familiariser avec une certaine terminologie.*
>
> - ***Présentation, tâche et projet d'étudiant***
>
> *Dans le cadre d'un cours, les étudiants peuvent produire des balados audio ou vidéo pour faire connaître leur projet et démontrer leur compréhension de la matière au reste de la classe.*
>
> - ***Faciliter l'apprentissage d'une langue seconde***
>
> *Un enregistrement d'une conversation ou un exercice de prononciation dans un cours aide l'étudiant dans son apprentissage d'une langue seconde.*
>
> - ***Fournir la rétroaction sur le travail d'un étudiant***
>
> *L'enseignant ou l'évaluateur enregistre la rétroaction sur l'évaluation d'un travail d'un étudiant.*

---

173 Kathleen Elliott VINSON, « What's on Your Playlist ? The Power of Podcasts as a Pedagogical Tool », (2009) 9 *Legal Studies Research Paper Series*, en ligne: <http://ssrn.com/abstract=1337737> (site consulté le 17 juillet 2010).

174 Wikibena, « Baladodiffusion », en ligne : <https://wiki.umontreal.ca/display/BENA/Utiliser+la+baladodiffusion#Utiliserlabaladodiffusion7.4%C3%89tapeIVRendrevotrebaladoreconnaissableentretous> (site consulté le 20 juillet 2010).

Cette technologie ne remplace pas un cours pédagogique, mais est un excellent complément à l'enseignement. L'usage de la baladodiffusion a plusieurs avantages[175] :

Avantages pour l'étudiant :

- ***Choisir le moment d'apprentissage***

L'étudiant peut choisir de revoir ses balados au temps et en lieu qu'il lui convient ou dans ses déplacements.

- ***Pallier une absence***

L'étudiant qui n'a pas pu être présent pour une raison ou autre peut accéder en différé au cours, à son cours tout en y percevant l'atmosphère.

- ***Améliorer sa compréhension***

L'étudiant qui n'a pas compris une partie du cours peut le réécouter à son rythme lui permettant de comprendre les explications de l'enseignant.

- ***Améliorer la prise de notes, la synthèse***

Regarder ou écouter le cours enregistré permet à l'étudiant d'en faire une synthèse ou de prendre de meilleures notes, dans le but d'améliorer progressivement sa prise de notes ou la rédaction d'une synthèse.

- ***Compléter ses connaissances***

L'étudiant peut accéder à des balados donnés par des experts, des sommités internationales sur un sujet disponible dans le cadre de son cours. Ces ressources l'aideront à compléter les connaissances acquises avec son enseignant.

- ***Visualiser des situations inaccessibles***

La baladodiffusion permet de démontrer des situations que l'étudiant rencontre rarement dû à des difficultés d'organisation comme une fouille en archéologie, ou à reproduire une manipulation délicate de chimie ou de physique, ...

Avantages pour l'enseignant :

- ***Améliorer sa prestation***

L'enseignant qui enregistre sa prestation en classe en balado vidéo peut profiter de l'occasion pour analyser son enseignement et l'améliorer.

- ***Valoriser son travail pédagogique***

La diffusion de ses cours en balado rend son travail pédagogique visible à l'extérieur, auprès d'un public plus large que celui de la classe. Ses qualités pédagogiques peuvent être diffusées et

---

175 Wikibena, « Baladodiffusion », en ligne : <https://wiki.umontreal.ca/display/BENA/Utiliser+la+baladodiffusion#Utiliserlabaladodiffusion7.4%C3%89tapeIVRendrevotrebaladoreconnaissableentretous> (site consulté le 20 juillet 2010).

reconnues au-delà des murs de l'établissement. Le chercheur peut profiter des balados pour diffuser le résultat de ses travaux de recherche lors de conférences, sur ses pages web, ...

- ***Produire un support pédagogique***

Le balado audio ou vidéo constitue un moyen de produire un support pédagogique animé.

- ***Mieux accompagner ses étudiants***

Le temps que l'enseignant économise en demandant aux étudiants de visionner ou d'écouter son cours en baladodiffusion, pourra être mis à profit pour renforcer l'accompagnement, le tutorat des étudiants. L'enseignant pourra consacrer plus de temps à la progression de ses apprenants.

- ***Devenir acteur de ses cours***

Le piratage devient inutile quand l'enseignant diffuse son cours en baladodiffusion. De cette façon, il permet à tout le monde d'accéder à son cours original. L'enseignant, en devenant acteur, contrôle ainsi la diffusion de son image, de sa voix et de sa pratique pédagogique.

2. Quels sont les risques associés à la baladodiffusion ?

Les risques des balados sont les mêmes que pour les autres environnements de diffusion et de partage de contenus dans les réseaux (l'utilisation non autorisée de l'image et de renseignements personnels; les atteintes au droit d'auteur; la présence de contenu illicite ou ne convenant pas aux enfants; les contenus haineux, menaçants, diffamatoires et contraires aux lois)

3. Comment évaluer ces risques ?

Pour évaluer les risques spécifiques à la diffusion et au partage de contenus au moyen de balados, il est opportun de s’interroger sur le public visé, la présence de sons, d’images ou de vidéos ainsi que les types d’informations concernées.

a. Le public visé

Le public cible visé module évidemment les attentes qu’une personne a en écoutant un balado. Ainsi, le contenu d’un fichier balado diffusé pour des enfants devra être approprié en fonction de leur âge. De plus, la diffusion d’un balado sur l’intranet d’une institution ne présente pas les mêmes risques que la diffusion du même fichier sur le Web en général. Les informations qui y seront contenues devront tenir compte du public auquel s'adresse le balado.

Question à vérifier *Quelles sont les personnes qui auront accès au balado ?*

b. La présence de sons, d'images ou de vidéos

La présence de matériel protégé par le droit d'auteur dans un balado augmente les risques pour un créateur. En effet, bien qu'un fichier balado soit une nouvelle création, la présence de tout matériel protégé ou sous licence peut engager la responsabilité de l'auteur qui l'a utilisé sans obtenir les autorisations nécessaires.

> ***Questions à vérifier***
> - *Retrouve-t-on du contenu sous droit d'auteur dans le balado ?*
> - *Si oui, a-t-on obtenu les autorisations nécessaires pour les utiliser dans le balado ?*
> - *Y a-t-il un mécanisme de licence mis en place et protégeant le fichier balado ?*

c. L'information contenue dans le fichier balado

Les fichiers balados peuvent traiter d'une multitude de sujets. Certains sont enregistrés dans des studios d'enregistrement de radios nationales, alors que d'autres sont créés à même des téléphones cellulaires de particuliers. L'accès à ces fichiers se fait de différentes façons selon qu'on souhaite télécharger le balado sur un MP3 ou sur un ordinateur personnel ou qu'on ne souhaite l'écouter qu'en lecture en transit.

De plus, les fichiers balados ne sont pas toujours accessibles à tous et sont parfois diffusés uniquement sur l'intranet d'une organisation. Dans d'autres cas, les baladodiffuseurs visent un large public et mettent en ligne des sujets aussi variés qu'une émission satirique de l'actualité, un bulletin de nouvelles, une chronique arts et beauté… Les sujets varient ainsi que les registres de langage. La qualité des informations qu'on y trouve varie tout autant que la forme du fichier. Il est facile pour une personne de créer son balado et d'y mettre tout le contenu qu'elle décide. Il faut donc faire preuve d'esprit critique et bien analyser la qualité et validité des informations reçues.

4. Quelles sont les précautions à prendre ?

a. Prévoir un moyen de dénoncer le contenu inapproprié

Bien que la dénonciation de contenu inapproprié ne soit pas le moyen le plus utilisé en matière de baladodiffusion, il pourrait être utile pour un site agrégateur – comme iTunes par exemple – de prévoir un moyen de signaler les atteintes aux droits ou la présence de contenu inapproprié dans un fichier balado.

b. Éviter de porter atteinte aux droits d'autres personnes

Il vaut toujours mieux demander la permission écrite des personnes créatrices des œuvres afin d'utiliser leur voix ou leur image dans un balado. On s'assure ainsi de ne pas attenter aux droits de tiers et l'on protège l'intégrité intellectuelle de notre œuvre. La règle générale veut que si l'on souhaite utiliser une partie ou la totalité de l'œuvre d'une autre personne (comme une œuvre musicale), l'on doive obtenir la permission de la

personne qui en détient les droits. Et cela est vrai que l'œuvre soit écrite, filmée ou musicale[176].

Dans le cas où l'obtention de permissions se révèle impossible, il peut être intéressant de vérifier si l'œuvre est protégée par une licence permettant l'utilisation partielle du matériel – comme la licence *Creative Commons*. Dans l'affirmative, il est important de regarder la catégorie de licence qui a été choisie et dans le cas où une protection minimale a été choisie par l'auteur, il pourrait être possible d'utiliser l'œuvre. Cela n'est toutefois pas une tendance générale pour l'ensemble des créations auxquelles on a accès et il est important d'assurer une vérification de chacun des fichiers que l'on souhaite utiliser. Sinon, le baladodiffuseur portera atteinte aux droits de tiers et pourra voir sa responsabilité engagée.

[176] Gavin SUTTER et Johanna GIBSON, « Podcasts and the law », 11 avril 2007, *JISC Legal Information.*

III. Les modèles de politiques, de mises en garde et de conseils

Mise en garde : Les modèles de politiques, de mises en garde et de conseils ne sont présentés qu'à titre d'exemples et ne sont pas conçus pour être utilisés tels quels. Comme nous l'avons vu tout au long de ce guide, les enjeux et les risques sont différents d'une situation à une autre et d'un site Web 2.0 à un autre. Les politiques doivent alors prendre en considération ces différences, ainsi que les caractéristiques du site Internet visé.

A. Politiques générales relatives à l'utilisation d'Internet

1. Politique d'utilisation du site Internet

Il est préférable pour chaque site Internet d'élaborer une politique d'utilisation spécifique pour informer les usagers des conduites qui sont tolérées ou non sur celui-ci. Voici un exemple de politique d'utilisation d'un blogue, qui peut être facilement adapté selon le type de site Web 2.0 visé :

> ***Expliquer le fonctionnement et les risques liés à l'utilisation du blogue;***
>
> ***Exemple** : Le blogue permet à une personne de créer facilement une page Web qui peut porter sur une diversité de sujet. Il se présente sous la forme de billets ou articles, publiés sur le site du plus récent jusqu'au plus ancien. Il est facile à mettre à jour et les visiteurs du site ont habituellement la possibilité de commenter les billets.*
>
> *Le blogue est accessible à un grand nombre de gens, il faut donc porter une attention particulière au contenu que l'on publie. Le blogueur sera tenu responsable du contenu qu'il publie sur son blogue, il peut être reconnu comme preuve valable pour établir un fait ou un acte juridique.*
>
> *Le blogue peut donner lieu à la transmission d'informations causant des préjudices à des personnes. Par imprudence, on peut révéler des éléments de la vie privée d'une personne, des propos peuvent porter atteinte à la réputation, des fichiers peuvent comporter l'usage non autorisé de l'image d'une personne. L'outil peut parfois être utilisé pour la harceler ou menacer.*
>
> ***Préciser les usages autorisés et les utilisations prohibées;***
>
> ***Exemple** : Le service d'hébergement de blogues doit être utilisé uniquement pour les fins suivantes : (--------décrire les finalités acceptées ou tolérées, par exemple, créer et administrer un blogue portant sur des sujets conformes avec la loi en vigueur-----------).*
>
> *Il faut éviter de révéler des informations sur des tiers, en particulier, il faut être prudent lorsqu'on publie un billet concernant des événements de notre vie privée. Il est toujours prudent de réviser un billet ou un commentaire avant de le publier.*
>
> *Il est interdit de transmettre du matériel haineux, pornographique ou harcelant ou à l'égard duquel on ne détient pas les droits d'auteur.*

Rappeler que l'usager peut être tenu responsable des propos publiés sur son blogue;

Exemple *: Sur Internet, l'usager dispose d'une grande maîtrise de ce qui lui est transmis ou de ce qu'il transmet. Personne n'est en mesure de l'empêcher de recevoir ou de diffuser de l'information s'il a vraiment envie de recevoir ou diffuser. En revanche, l'individu est le premier responsable de ce qu'il reçoit ou de ce qu'il transmet sur Internet.*

En dépit de la grande liberté que le réseau Internet laisse aux personnes, il existe dans tous les pays des lois délimitant ce qui peut ou non être transmis, reçu ou possédé par les personnes. Chaque usager a l'obligation de respecter ces lois. Sinon, de lourdes sanctions peuvent lui être imposées.

Rappeler les principes de respect des droits des personnes;

Le droit à la vie privée

Exemple *: Toute personne a droit au respect de sa vie privée. Il est ainsi interdit de porter atteinte à la vie privée d'une personne.*

Par exemple, on ne doit pas révéler des éléments de l'intimité d'une personne comme sa vie personnelle et familiale (ex : vie sentimentale ou sexuelle, son état de santé, sa vie familiale, son domicile, ses opinions politiques, religieuses ou philosophiques, son orientation sexuelle, son anatomie, son intimité corporelle...)

Le droit à la réputation des personnes

Exemple *: Toute personne a droit au respect de sa réputation. Il est ainsi interdit de porter atteinte à la réputation d'une personne, en l'exposant à la haine ou au mépris et en lui faisant perdre l'estime ou la confiance des autres à son égard.*

Par exemple, affirmer ou insinuer des faits sur une personne d'une façon négligente ou téméraire, sans avoir d'abord vérifié la véracité des propos. Ou encore, s'agissant de faits véridiques, les rappeler sans motif légitime dans le seul but de nuire, ridiculiser, humilier, injurier ou insulter une personne.

Le droit à l'image des personnes

Exemple *: Il est interdit de capter ou de diffuser l'image ou la voix d'une personne lorsqu'elle se trouve dans un lieu privé sans son consentement. Lorsque la personne se trouve dans un lieu public, il est conseillé fortement d'obtenir son consentement à la diffusion, surtout s'il est possible de l'identifier.*

Par exemple, envoyer, via une liste de diffusion, une photo d'une personne sans son autorisation, diffuser la photo d'une personne sur un site web ou un blogue sans son autorisation, diffuser sur Internet une vidéoconférence sans l'autorisation des participants...

Expliquer comment le droit d'auteur s'applique aux informations trouvées sur l'Internet;

Exemple *: La plupart des textes, images, dessins, sons, œuvres musicales que l'on trouve sur Internet sont protégés par le droit d'auteur.*

Le droit d'auteur est le droit exclusif de décider de diffuser, de reproduire ou autrement communiquer une œuvre au public, de la publier, de l'adapter, de la traduire.

Sauf lorsque cela est explicitement mentionné, on ne doit jamais prendre pour acquis que l'on peut copier, reproduire et diffuser quelque contenu que ce soit qui se trouve sur Internet. Il faut, en général, demander l'autorisation pour reproduire et diffuser une œuvre, par exemple, sur une page web ou dans une liste publique de discussion.

Rappeler les principes de respect des lois d'ordre public;

Il s'agit ici d'expliquer que des lois existent afin de prévenir des conflits ou des comportements qui sont considérés comme contraires aux valeurs de notre société. Il en est ainsi pour les informations à caractère pornographique, la propagande raciste et l'incitation à la haine.

Propagande haineuse

***Exemple** : Il est interdit de tenir des propos qui constituent de la propagande haineuse. La propagande est une action exercée sur l'opinion pour l'amener à adopter certaines idées politiques, sociales ou autres; elle sera dite haineuse lorsqu'elle vise à créer une aversion profonde contre certains groupes de personnes.*

Par exemple, préconiser l'extermination des membres d'un groupe à cause de leur couleur, de leur race, de leur religion, de leur origine ethnique ou de leur orientation sexuelle; communiquer publiquement des déclarations (par des mots, parlés, écrits ou enregistrés, des gestes ou des signes) qui incitent à la haine contre un groupe se différenciant par sa couleur, sa race, sa religion, son origine ethnique ou son orientation sexuelle et qui sont susceptibles d'entraîner une violation de la paix; communiquer des propos, autrement que dans une conversation privée, qui encouragent ou essaient de convaincre les gens de haïr un groupe identifiable par la couleur, la race, la religion, l'origine ethnique ou l'orientation sexuelle.

La propagande haineuse diffère des propos exprimant des opinions légitimes à l'égard de groupes, de religions ou d'entités.

Matériel obscène

***Exemple** : Le matériel obscène, c'est-à-dire le matériel qui exploite les choses sexuelles de façon dégradante ou déshumanisante, n'est pas toléré dans notre société. Ce matériel doit être proscrit, et ce, même en l'absence de cruauté et de violence.*

Pornographie juvénile

***Exemple** : La pornographie juvénile s'entend de représentations graphiques, photographiques, filmées, vidéos ou autres, réalisées ou non par des moyens mécaniques ou électroniques de mineurs se livrant à des activités explicitement sexuelles.*

L'utilisation d'Internet pour communiquer avec un enfant dans le but de commettre une infraction sexuelle contre cet enfant ou pour transmettre, rendre accessible, exporter de la pornographie juvénile ou d'y accéder constituent des infractions. La loi permet aux tribunaux d'ordonner la suppression de la pornographie juvénile affichée sur un

ordinateur canadien et permet la confiscation de matériels ou d'équipements utilisés pour commettre une infraction.

Préciser les conséquences d'un comportement indésirable;

Exemple *: Le site d'hébergement de blogues se réserve le droit de fermer un blogue qui serait contraire à la présente politique ou de bloquer le compte d'une personne ne s'y conformant pas.*

2. Politique de protection de la vie privée

Voici un exemple de politique de protection de la vie privée compatible avec la *Loi sur la protection des renseignements personnels dans le secteur privé*[177], qu'il est possible d'intégrer à un site Web 2.0 :

Objet

Nous sommes particulièrement attentifs à préserver la confidentialité des données des usagers qui utilisent ce site. Ainsi, aucune donnée nominative n'est présente sur ce site. Par ailleurs, dans la conduite de nos opérations, nous nous efforçons de respecter en tout temps la confidentialité de vos données personnelles, et ce, en accord avec la politique de protection de la vie privée qui suit.

Information recueillie lors de la fréquentation du site

- *Information obtenue lors de l'inscription*

Lors de l'inscription, certaines données seront requises pour pouvoir s'abonner au site Internet. Elles ne seront en aucun cas divulguées à un tiers.

- *Information obtenue lors de votre accès au site*

Comme pour tout site web, les serveurs qui hébergent nos sites identifient l'adresse Internet (IP) de votre connexion Internet afin de permettre l'échange de données entre nos serveurs et votre ordinateur. Aucune information permettant de vous identifier n'est associée à votre adresse IP.

- *Informations obtenues par les « fichiers-témoins » (cookies)*

Les « cookies » ou fichiers témoins sont de petits fichiers texte qui sont téléchargés sur votre disque dur lorsque vous visitez certaines pages web. Ces fichiers sont inoffensifs pour votre ordinateur sur lequel vous avez le plein contrôle. Nos serveurs utilisent ces témoins afin de personnaliser l'affichage des pages et afin de recueillir certaines statistiques d'utilisation de nos sites. Il vous est cependant possible en tout temps de modifier la configuration de votre ordinateur ou de votre logiciel fureteur et de ne plus accepter le téléchargement des cookies.

---

[177] L.R.Q., c. P-39.1

Finalité de la collecte d'information

L'information obtenue lors de l'inscription au site Internet n'est nécessaire que pour avoir accès aux différentes sections du site. L'information concernant l'adresse IP n'est utilisée que pour permettre l'échange de données entre nos serveurs et votre ordinateur. L'information obtenue par les fichiers-témoins est utilisée pour personnaliser l'affichage des pages Internet.

Communication de l'information

Les données recueillies par le site Internet ne seront en aucune façon communiquées à des tiers, que ce soit dans le cadre d'une liste de diffusion ou dans le cadre d'un concours promotionnel. Elles pourront toutefois être divulguées lorsque la loi nous en oblige.

Détention et sécurité des données

Les données recueillies seront conservées sur les serveurs du site Internet pour la période nécessaire à la réalisation des finalités mentionnées. Ces données seront protégées et les employés n'y auront pas accès.

Accès à votre dossier

Vous pouvez en tout temps consulter ou rectifier les données vous concernant en nous contactant par courrier électronique à l'adresse suivante : (inscrire l'adresse de courrier électronique).

3. Politique de gestion du droit d'auteur et des autres propriétés intellectuelles

Voici un exemple de politique de gestion du droit d'auteur et des autres propriétés intellectuelles :

Exemple :

La propriété intellectuelle fait référence à la protection des droits d'un auteur sur une œuvre qu'il a créée, écrite ou exprimée. La propriété intellectuelle inclut la protection des droits d'auteur, des marques de commerce ainsi que des inventions. Dans la poussée actuelle du développement des nouvelles technologies de l'information, où la reproduction éphémère et l'enregistrement digital sont la norme, le concept de la propriété intellectuelle est devenu fondamental. L'Internet, le courriel et les pages web fournissent de multiples forums permettant la création de graphiques, de textes, d'œuvres d'art et de musique en plus des multiples opportunités pour les tiers de se les approprier. Certaines solutions techniques s'offrent à l'usager désireux de protéger ses œuvres.

Il convient toutefois de toujours avoir à l'esprit que :

- *Les images, textes et créations trouvés sur l'Internet sont la propriété de leur créateur. Tout usage de telles œuvres nécessite l'autorisation de leur auteur.*

- *L'utilisation, la publication et la retransmission de la musique, des images, des textes, des pages web et autres informations trouvées sur l'Internet sont soumises aux restrictions énoncées dans la loi sur le droit d'auteur.*
- *Le piratage de logiciel, la reproduction sur CD-Rom ou par retransmission sont des actes interdits par la loi.*

Le contenu publié sur le site Internet qui est en contravention avec les lois sur le droit d'auteur sera retiré du site, et ce, sans aucun préavis.

B. Politiques et précautions spécifiques selon le type de site Web 2.0 utilisé

1. Les blogues

a. La Nétiquette[178]

Pour rendre plus agréable la navigation sur un blogue, il convient d'adopter une nétiquette qui mentionne les comportements qui ne sont pas tolérables sur le blogue ainsi que les règles de savoir-vivre. Elle s'applique autant pour les blogueurs que pour ceux qui publient des commentaires. Ces règles ont été établies avec l'usage par les blogueurs et en voici des exemples :

- Ne pas employer un langage vulgaire, menaçant, diffamant, insultant ou faire des commentaires racistes, à connotation ethnique ou contraire à la loi.
- Les commentaires à caractère pornographique et la publicité ne sont pas acceptés.
- Respecter en tout temps le droit d'auteur et mentionner la source exacte lorsque des citations ou des extraits d'une œuvre sont employés.
- Éviter les mots écrits en majuscule, cela donne l'impression de crier.
- Ne pas publier de commentaire anonyme. L'utilisation d'un pseudonyme est acceptée, mais il faut fournir une adresse de courriel valide.
- Pour résoudre un conflit qui s'amplifie, il faut essayer de le faire en privé avant de publier des commentaires.

---

178 Pour voir des exemples de nétiquettes qui ont été adoptées : LES HUMAINS ASSOCIÉS, *Une nethique pour le blog 1.0*, en ligne : <http://nethique.info/charte>; Mario TOUT DE GO, *Politique éditoriale de « Mario, tout de go »*, en ligne : <http://carnets.opossum.ca/mario/archives/2003/07/politique_edito.html>; Tom O'REILLY, *Draft Blogger's Code of Conduct*, en ligne : <http://radar.oreilly.com/archives/2007/04/draft_bloggers_1.html>; BLOGHER, *What are your community guidelines ?*, <http://blogher.org/community-guidelines>.

Pour une version Wiki de la nétiquette en français, voir le site Blogging Wikia : *Code de conduite pour la blogosphère par Tim O'Reilly*, en ligne : <http://blogging.wikia.com/wiki/Code_of_conduct_in_French>.

2. Les sites de partage de contenu

Pour les sites de partage de contenu, il peut être nécessaire de reprendre la politique de gestion du droit d'auteur et des autres propriétés intellectuelles et de la mettre plus en évidence sur le site Internet. En effet, la violation du droit d'auteur est un des risques les plus importants sur les sites de partage de contenu.

3. Les sites de réseaux sociaux

a. Les conseils de sécurité[179]

Pour minimiser les risques que représentent les sites de réseautage social, il peut être important de mettre en ligne des conseils de sécurité. Lorsque les usagers sont des enfants, il peut être utile de parler avec eux de ces règles et de convenir qu'elles seront respectées.

- Ne pas oublier que le site de réseautage social est un endroit public. Par conséquent, il est prudent de ne pas révéler une information que nous ne voudrions pas que tout le monde connaisse.
- Il faut éviter de révéler des informations personnelles nous concernant. Des renseignements tels notre adresse, notre nom complet, notre numéro de téléphone, notre date de naissance ou encore notre numéro d'assurance-sociale ne devrait pas être communiqué.
- De la même façon, nous ne devrions pas publier des informations que nous ne voudrions pas dévoiler à notre employeur ou encore à nos parents. En effet, ceux-ci peuvent parfois naviguer sur le site et voir ces renseignements. Si nous ne voulons pas qu'ils les voient, c'est un indice que nous ne devrions peut-être pas publier le contenu en question.
- Il est prudent d'accepter seulement sur notre liste de contact les gens que nous connaissons bien. En effet, cela évite qu'un profil mis à la disposition des amis exclusivement puisse être vu par des inconnus.
- Les usagers des sites de réseautage social ne sont pas toujours les gens qu'ils prétendent être. Il faut donc être prudent avant de dévoiler à quelqu'un des éléments de notre vie privée ou de faire des confidences. De plus, nous ne devrions pas rencontrer des personnes inconnues. Dans le cas contraire, le rendez-vous devrait être pris dans un endroit public et en présence d'une personne de confiance, comme un parent.

---

179 Pour voir des exemples de conseils de sécurité qui ont été adoptés : MYSPACE, *MySpace Safety Tips*, en ligne : <http://www.myspace.com/error?ETOID=0&EC=404#!/help/safety/tips>; WIRED SAFETY, *Parry Aftab's Guide to Keeping Your Kids Safe Online*, en ligne : <http://www.wiredsafety.org/resources/pdf/socialnetworktips.pdf>; WINDOWS LIVE SPACES, *Sécurité*, en ligne : <http://explore.live.com/hotmail-security>.

- Si nous sommes mal à l'aise face au comportement d'un usager, que ce soit parce qu'il propage des menaces, qu'il met en ligne des photographies de nous ou qu'il incite à des actes sexuels, il ne faut pas hésiter à le dénoncer.
- Les messages non sollicités à connotation sexuelle devraient être complètement ignorés. Ces propos devraient par contre être rapportés aux administrateurs du site et/ou à une personne de confiance.

4. Les sites d'évaluation de personnes, de services ou de produits

a. Les conseils d'écriture de commentaires[180]

Pour rendre plus agréable la navigation sur les sites d'évaluation de personnes, de produits ou de services, il convient d'adopter des règles concernant l'écriture des commentaires sur le site. Ces règles mentionnent les types de propos qui sont tolérés ou non sur le site, dans le but d'éviter, entre autres, que des commentaires déplacés ou illicites soient publiés. Ces règles ont été établies avec l'usage par les usagers et en voici des exemples :

> - *Il faut laisser des évaluations et des commentaires utiles.*
> - *Ne pas employer un langage vulgaire, menaçant, diffamant, insultant ou faire des commentaires racistes, à connotation ethnique ou contraire à la loi.*
> - *Les commentaires à caractère pornographique et la publicité ne sont pas acceptés.*
> - *Il faut se limiter à un seul commentaire par personne.*
> - *Il est interdit de publier plusieurs évaluations dans le but de hausser la réputation ou la note de quelqu'un ou quelque chose.*
> - *Ne pas inclure des informations personnelles en publiant un commentaire qui pourrait permettre d'identifier l'auteur du commentaire.*

---

180 Pour voir des exemples de conseils d'écriture qui ont été adoptés : RATEMYPROFESSORS, *Posting Guidelines*, en ligne : <http://www.ratemyprofessors.com/rater_guidelines.jsp>; AMAZON, *Conseils d'écriture pour les commentaires d'internautes*, en ligne : <http://www.amazon.fr/gp/customer-reviews/guidelines/review-guidelines.html/171-0464676-0020242 ?ie=UTF8&asin=2266136046>; AMAZON, *Review Writing Guidelines*, en ligne : <http://www.amazon.ca/gp/help/customer/display.html/701-71595490978746 ?ie=UTF8&nodeId=1057790&asin=2266104535>; EBAY, *Retrait d'évaluations et évaluations illégales*, en ligne : <http://pages.cafr.ebay.ca/help/policies/feedback-abuse-with drawal.html>.

5. Les sites Wikis

a. La Nétiquette[181]

Pour rendre plus agréable la navigation sur les sites Wikis, il convient d'adopter une nétiquette qui précise les comportements non tolérés sur le site ainsi que les règles de savoir-vivre. Ces règles ont été établies avec l'usage par les contributeurs et en voici des exemples :

- *Ne pas employer un langage vulgaire, menaçant, diffamant, insultant ou faire des commentaires racistes, à connotation ethnique ou contraire à la loi.*
- *Les commentaires à caractère pornographique et la publicité ne sont pas acceptés.*
- *Respecter en tout temps le droit d'auteur et mentionner la source exacte lorsque des citations ou des extraits d'une œuvre sont employés.*
- *Éviter le plus possible les fautes d'orthographe, en particulier les abréviations utilisées pour d'autres moyens de communication comme le clavardage.*
- *Éviter de publier des articles de façon anonyme. L'utilisation d'un pseudonyme est acceptée, mais il faut fournir une adresse de courriel valide.*
- *Pour résoudre un conflit qui s'amplifie, il faut essayer de le faire en privé ou sur la page de discussion reliée à l'article en question. Les modifications incessantes de l'article pour effacer le travail de l'autre sont prohibées.*

---

181 Pour voir des exemples de nétiquettes qui ont été adoptées : RS2I.NET, *Netiquette*, en ligne : <http://www.rs2i.net/wiki/Netiquette>; WIKIPEDIA, *Wikipedia : Etiquette*, <http://en.wikipedia.org/wiki/WP:Wikiquette>.